YOUNG AMERICAN CONSUMERS' PRIOR NEGATIVE EXPERIENCE OF ONLINE DISCLOSURE, ONLINE PRIVACY CONCERNS, AND PRIVACY PROTECTION BEHAVIORAL INTENT

Hongwei (Chris) Yang, Appalachian State University

ABSTRACT

A web survey of 403 American college students generated data which permitted the testing of a model of the effects of prior negative experience of online disclosure on the students' online privacy protection intentions. It showed that young American consumers' prior negative experience of online disclosure: directly increased their online information privacy concerns; heightened their risk perceptions of online disclosure; undermined their trust in online companies, Internet marketers and laws to protect online privacy; reduced their time spent on SNS; and enhanced their intent to falsify personal information and/or to refuse to provide personal information. Students' online privacy concerns mediated the impact of prior negative experience on their: intention to refuse information provision; asking for removal of their personal information; spreading negative eWOM; and complaining to online companies. Students' online privacy concerns were found to elevate their perceived risks and undermined their trust in online companies, marketers and laws to protect privacy. Results provide online companies and Internet marketers some valuable insights on how poor customer relationship management might compromise precise, targeted marketing in social media.

INTRODUCTION

The phenomenal success of social networking websites (SNS), especially Facebook, depends on SNS subscribers' voluntary disclosure of enormous amounts of personal information. SNS make huge profits by utilizing the users' profiles, status updates, and social connections as well as their friends' recent activities for advertising and marketing purposes (Quinn 2010). SNS allow advertisers to tailor their ads more effectively and target to social media users more precisely, especially those who express brand preferences and interests on SNS. In addition, SNS sites also generate revenues by supplying mountains of their subscribers' personal information to marketers, recruiters and any interested party. As a result, eMarketer (2012ab) estimated that U.S. marketers would spend about $3.63 billion to advertise on SNS and Facebook alone will receive $6.1 billion from advertisers worldwide in 2012.

However, the inappropriate collection, use, and dissemination of online personal data might curb consumers' enthusiasm for sharing valuable personal information on SNS, diminish the effectiveness of targeted social ads, hinder online bonding between brands/companies and customers, and attract regulators' attention. There exists an abuse of SNS subscribers' disclosed privacy information for the purposes they did not approve of (FTC 2010).

Very recently, there are some ominous signs that the effectiveness of social media advertising is eroding. Wall Street Journal reported that General Motors decided to withdraw its Facebook ads because they had little impact on consumers' car purchases (Terlep, Vranica and Raice 2012). *Advertising Age* reported that Facebook had been busy introducing new advertising models and metrics to prove its worth to advertisers, due to the dismal click-through rate of Facebook ads and marketers' general doubts over Facebook advertising effectiveness (Hof 2011). One probable explanation is that Facebook ads were not fed to Facebook users based on truthful and accurate personal information they disclosed so that most of Facebook ads were dismissed as irrelevant and uninteresting. In light of advertisers' doubts on the effectiveness of social media advertising, more empirical studies about consumer behavior of privacy disclosure and protection can provide interactive marketers and online companies valuable insights and guidance for improving their management of marketing communications in social media.

Meanwhile, parents, consumer advocacy groups, and the government have become increasingly concerned about the extent and nature of young American consumers' personal information disclosed on SNS whose design is

inherently open but vulnerable. Published research shows that a majority of college students disclose their lifestyle information such as favorite books, music, interests, their dating preferences, relationship status, and political views while a considerable number of them (16-40%) list a phone number and many of them even share their birthday (Acquisti and Gross 2006; Gross and Acquisti 2005; Jones and Soltren 2005; Stutzman 2006). On the other hand, security, access controls, and privacy are weak by design on most SNS because their popularity and commercial value hinge upon their easy and open access to all Internet users (Shin 2010). In addition, SNS themselves are vulnerable to various attacks from hackers and cyber predators who covet subscribers' personal data (Chen and Shi 2009). Consequently, the online behavioral advertising practices of SNS are facing the increasing scrutiny of the congress and the Federal Trade Commission (FTC) as they extend beyond what the SNS users originally intended: to develop and maintain social connections (Hoy and Milne 2010). After Facebook launched its "Open Graph Platform" that extends the social net's web across third-party sites, New York Senator Charles Schumer sent a letter to the Federal Trade Commission asking to develop guidelines for how Facebookers' information can be used and called a press conference with three other senators (Learmonth 2010). The FTC (2010) recently endorsed "Do Not Track" legislation to establish a uniform and comprehensive mechanism to protect consumers who do not want to be tracked or receive targeted advertisements.

Adolescents and young adults are the heaviest users of SNS but little is known about their online privacy protective behaviors in relation to their social media use. Two Pew Internet Project surveys show that 73% of online teens and 72% of young adults use SNS (Lenhart et al. 2010). Popular media and trade press have been voicing the concerns of government and privacy advocacy groups while also creating a myth that teenagers and young adults do not care about their online privacy at all (Dvorak 2010; O'Brien 2010). On the other hand, a new trend has been noted that more and more young college students are beginning to rethink online privacy and to exercise control over their personal information on SNS (Holson and Helft 2010). Another Pew study indicates that 71% of SNS users ages 18-29 had changed the privacy settings on their profile to limit what they share with others online (Madden and Smith 2010). Another quantitative study also concludes that young people ages 18-24 have an aspiration for increased privacy like older Americans (Hoofnagle et al. 2010). However, few researchers have examined the relationship between online privacy concerns and privacy protection behaviors among young American consumers ages 18-29.

Current social media research in top advertising and marketing journals heavily focuses on social media as advertising/marketing tools. The majority of previous advertising and marketing studies concerns social media usage, perception, and attitude towards social media (Khang, Ki and Ye 2012). Few studies have addressed the consequences or effects of online companies and Internet marketers' misuse or abuse of social media users' personal data and the dynamic relationships between consumers' prior negative experience of online disclosure, online privacy concerns, perceived risk, trust, social media use, and their privacy protection intents on SNS. Hence, many important questions remain unanswered. For example, are young American consumers protecting their online privacy? Is their online privacy protection proactive or reactive? Does their social media use loosen their self-protection of online privacy? What are managerial implications of their behavior of online privacy disclosure and protection?

Before government agencies, consumer advocacy groups and industry agree upon an effective regulatory mechanism of social media marketing, they need to know whether young American consumers are worried about online privacy and to what extent their prior negative experience of online disclosure influences their online privacy concerns, perceived risk, trust, social media use, and intent to adopt online privacy protective behaviors. The call for stricter government regulation of SNS privacy practices is very justified if young American Internet users seriously care about the collection and uses of their online personal information but they seldom take action to protect their own online privacy. Self-regulation will be more appropriate if most of young American consumers are genuinely concerned about online privacy, and intend to adopt six effective measures to defend their privacy rights in the cyberspace. Hopefully, online marketers and social media companies will improve marketing practices such as customer

relationship management (CRM) after learning new insights of the impact of young American consumers' prior negative experience of online disclosure, online privacy concerns, trust, risk, and social media use on their privacy protection intent.

Against this backdrop, the current study constructs and tests a conceptual model to further our understanding of young American consumers' behavior of online privacy disclosure and protection.

THEORETICAL FRAMEWORK

Online Information Privacy Concerns

Previous studies show that consumers' online privacy concerns are multi-dimensional and complicated, and various online marketing activities may evoke varying levels of concern (FTC 1998). Smith et al. (1996) found that *collection* becomes consumers' concern when they perceive that "extensive amounts of personally identifiable data are being collected and stored in databases." Consumers are also concerned about *unauthorized secondary use*, that is, "information is collected for one purpose but is used for another, secondary purpose." *Improper access* bothers consumers when "data about individuals are readily available to people not properly authorized to view or work with this data." Consumers also worry about *error* because "protections against deliberate and accidental errors in personal data are inadequate" (Smith et al. 1996, p. 172). Smith and associates developed a scale to measure these dimensions and validated it across the populations of students, consumers, and professionals. The validity and reliability of this instrument have been confirmed by subsequent empirical studies (e.g., Milberg, Smith, and Burke 2000; Rose 2006; Stewart and Segars 2002). Further research also supported unauthorized secondary use, improper access and error as legitimate consumers' online privacy concerns (e.g., Janda and Fair, 2004; Metzger and Doctor, 2003; Sheehan and Hoy, 2000; Shin, 2010).

Therefore, in the current study, consumers' online privacy concerns are conceptualized as the degree to which an online consumer is concerned about the collection of online personal information, unauthorized secondary use, improper access, and error. Online information privacy concerns will be treated as a multi-dimensional construct and a second-order factor as have other scholars (e.g., Stewart and Segars 2002; Malhotra et al. 2004; Okazaki, Li, and Hirose 2009).

Social Contract Theory

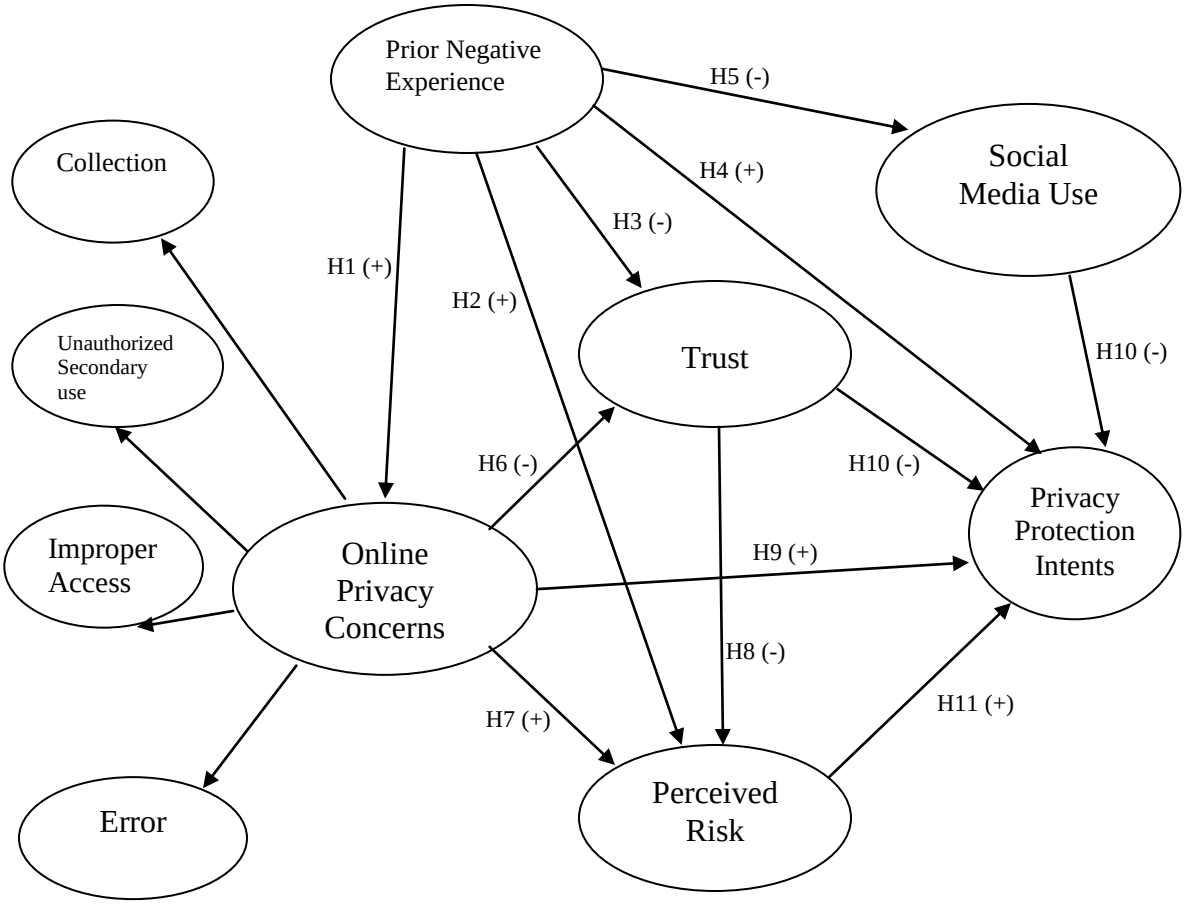
Social contract theory will be adopted to explain the underlying dynamics of how young American consumers' prior negative experience and online privacy concerns work together to influence perceived risk, trust, social media use, and six privacy protection behaviors examined in this study. Social contract theory has been applied by several marketing scholars to examine consumers' privacy concerns in both offline and online contexts (e.g., Culnan and Bies 2003; Malhotra et al. 2004; Phelps, Nowak, and Ferrell 2000; Okazaki et al. 2009). Other studies also consider consumers' exchange of personal information with marketers as an implied social contract (e.g., Culnan 1995; Milne 1997; Milne and Gordon 1993).

From this perspective, a social contract is formed whenever a consumer provides a marketer with personal information on the Internet in exchange for any incentive (including free convenient services of SNS). The consumer expects that their personal information will be managed responsibly. The implied contract will be regarded as "fair" if the marketer complies with FTC's five fair information practice principles of notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress, and if the consumer has reasonable control over their personal information collected by the marketer (Culnan 1995). The contract will be breached by the marketer if a consumer's personal information is collected without his knowledge or consent, if his personal information is provided to a third party without permission, if his personal information is used for any other purpose not agreed upon by him, if the accuracy of his personal data is not safeguarded, if he is not offered an opportunity to opt out, or if he is not informed of the firm's privacy policy (Phelps et al. 2000). So, when none of the above improper behavior occurs, consumers' privacy is protected but when consumer control is lost or reduced involuntarily after and beyond a marketing transaction, his privacy will be invaded (Culnan 1993; Milne and Gordon 1993).

Based on the social contract theory and the current literature, a conceptual model of privacy protection behaviors in social media is proposed as shown in Figure 1. The sections following provide the rationale for 11 causal paths in the proposed model.

FIGURE 1

The Proposed Model of Prior Negative Experience and Privacy Protection



Prior Negative Experience and its Consequences

Previous studies have shown that prior negative experience in personal information disclosure can significantly increase consumers' information privacy concerns in both online and offline contexts (e.g., Bansal et al. 2010; Culnan 1993; Okazaki et al. 2009). In turn, consumers' online privacy concerns hinder consumer's participation in Internet marketing and e-commerce (Sheehan and Hoy 1999; Cho and Cheon 2004).

After a prior negative experience of online disclosure, consumers perceive that an implied social or psychological contract has been breached by online companies or Internet marketers. Consequently, dissatisfied consumers feel riskier providing personal information online and they will be less likely to trust that online companies or Internet marketers will handle their disclosed online data in good faith. Research

shows that the psychological contract violation of individual online merchants considerably damages Internet users' trust in the community of online sellers (Goles et al. 2009; Pavlou and Gefen 2005). Accordingly, prior negative experience of online privacy invasion can not only heighten consumers' risk perception of online disclosure directly (e.g., Bansal et al. 2010) but also undermine their trust in online companies or Internet marketers or laws to protect online privacy.

Some studies indicate that consumers' past experience of information disclosure to marketers serves as a strong predictor of their willingness to reveal personal information to marketers (Culnan and Armstrong 1999; Metzger 2006). On the other hand, prior negative experiences of online disclosure should force consumers to take protective measures such as withholding or falsifying personal information. For example, consumers victimized by privacy invasion tend to refuse to be profiled online for personalized advertising (Award and Krishnan 2006) and Facebook users with past experiences of privacy invasion tightened their privacy settings (Debatin et al. 2009).

The existential value of SNS is information sharing with friends, relatives and acquaintances (Ellison et al. 2007; Shin 2010). When young American consumers begin to worry about their online privacy due to prior negative experience, they will be more reluctant to disclose accurate personal information on SNS and naturally, their time spent on SNS will be reduced. Therefore, the following research hypotheses are proposed:

H1: Young American consumers' prior negative experience of online disclosure increases their online information privacy concerns.

H2: Young American consumers' prior negative experience of online disclosure increases their perceived risk of online disclosure.

H3: Young American consumers' prior negative experience of online disclosure undermines their trust of online companies, Internet marketers and laws to protect online privacy.

H4: Young American consumers' prior negative experience of online disclosure positively predicts their intent to (a) refuse information provision; (b) falsify personal information; (c) request the removal of personal information; (d) spread negative eWOM; (e) complain to online companies; and (f) report to the authorities.

H5: Young American consumers' prior negative experience of online disclosure reduces their time spent on SNS.

Online Privacy Concerns, Trust and Risk

In this study, trust refers to the degree to which Internet users believe online companies, marketers, and laws are dependable in protecting consumers' personal information (Malhotra et al. 2004). In addition, Internet users reasonably expect that online companies and marketers will abide by privacy laws and use their disclosed personal information only for the approved purpose(s). From a social contract perspective, when parties are involved in a contractual relationship, one party must assume that the other will act responsibly to fulfill its promises (Okazaki et al. 2009).

Some research shows that addressing consumers' online privacy concerns helps build their trust of online companies (e.g., Rifon et al. 2005). However, Metzger (2004) found that Internet users' privacy concerns negatively influenced their trust in websites. Similarly, other studies have revealed that consumers' information privacy concerns negatively affected their trust in online companies' commitment to protect their personal information (e.g., Malhotra et al. 2004) and their trust in mobile advertisers' proper handling of their personal information (Okazaki et al. 2009). Hence, it is posited that

H6: Young American consumers' online privacy concerns negatively affect their trust in online companies, marketers and laws to protect online privacy.

Perceived risk is conceptualized as the extent to which Internet users are uncertain about the negative consequences of providing personal information to online companies and marketers (Okazaki et al. 2009; Pavlou 2003). Because of the impersonal and distant nature of e-commerce and Internet marketing, Internet users feel at the risk that online companies will behave in an opportunistic manner by mishandling their personal information. In addition, considering various security threats to online companies' databases, Internet users are also uncertain whether their personal information will be leaked, breached, or stolen by hackers (Pavlou 2003). Several studies have provided empirical evidence that consumers' perceived risk will be exacerbated by their elevated information privacy concerns (e.g., Malhotra et al. 2004; Okazaki et al. 2009). It is therefore reasonable to expect that

H7: Young American consumers' online privacy concerns positively increase their perceived risk in disclosing personal information online.

Previous studies also suggest that trust can mitigate consumers' perceived risk of disclosing personal information to direct marketers and conducting online transactions and thus reduce the uncertainty of participating in e-commerce and interactive marketing activities (Jarvenpaa et al. 1999; Malhotra et al. 2004; McKnight et al. 2002; Okazaki et al. 2009; Pavlou 2003). So, the following research hypothesis is proposed:

H8: Young American consumers' increased trust in online companies, marketers and laws decreases their perceive risk of disclosing personal information online.

Online Privacy Concerns, Trust, Risk and Privacy Protection

Consumer studies have found consistently a positive relationship between the level of privacy concerns and protection behaviors. Sheehan and Hoy (1999) revealed that when online consumers' privacy concerns were heightened, they were more likely to provide incomplete information to online companies, to notify Internet Service Providers (ISPs) about unsolicited e-mail, to request name removal from lists, to send flames, and to abstain from using some websites. Similarly, Milne et al. (2004) identified level of privacy concerns as a strong predictor of online privacy protection behaviors including refusing to provide information, supplying false or fictitious information, asking for the removal of personal information, and refraining from using a website. Further studies have confirmed that consumers' online privacy concerns influenced their behavioral responses such as falsifying information, refusing information disclosure or transactions, or removing personal information from lists (Lwin et al. 2007; Wirtz et al. 2007). Similar behavioral patterns were discovered among teenagers (e.g., Moscardelli and Divine 2007; Youn 2005; 2009).

Thus, it is proposed that:

H9: Young American consumers' online privacy concerns positively predict their intent to (a) refuse information provision; (b) falsify personal information; (c) request the removal of personal information; (d) spread negative eWOM; (e) complain to online companies; and (f) report to the authorities.

The current literature suggests that trust can be built to reduce consumers' risk perceptions and encourage their use of ecommerce and Internet marketing (e.g., Cases 2002; Comegys et al. 2009; Miyazaki and Fernandez 2001; Pavlou 2003). Trust will be gained if online companies and Internet markers act responsibly and comply with the FTC self-regulatory rules. In turn, consumers will be more likely to trade their personal information for the communication benefits of SNS. Previous studies show that consumers' trust of online companies and marketers is positively associated with their behavioral intent to disclose personal information online (Joinson et al. 2010; Malhotra et al. 2004; Metzger 2004; Rifon et al. 2005). Correspondingly, trusting consumers will be less likely to adopt online privacy protection measures.

So, the present study posits that

H10: Young American consumers' trust in online companies, marketers and laws to protect online privacy negatively predicts their intent to (a) refuse information provision; (b) falsify personal information; (c) request the removal of personal information; (d) spread negative eWOM; (e) complain to online companies; and (f) report to the authorities.

Past studies indicate that perceived risk inhibits Internet users from engaging in online transactions and marketing activities (e.g., Cases 2002; Comegys et al. 2009; Miyazaki and Fernandez 2001; Pavlou 2003). Similarly, when consumers are concerned about the mishandling of their online personal information, they will be deterred from disclosing personal information on SNS. Marketing researchers found that perceived risk negatively affected Internet users' willingness to disclose valuable personal information to online companies and marketers (e.g., LaRose and Rifon, 2007; Malhotra et al., 2004; Myerscough et al., 2006; Norberg et al., 2007; Olivero and Lunt, 2004).

Consequently, Internet users will be more likely to engage in privacy protection behaviors to mitigate their risk perceptions. Rogers (1975) argues that the likelihood and severity of perceived risk motivate one's self-protection behavior. Recent studies have confirmed that perceived risk of online disclosure lead to consumers' adoption of privacy protection behaviors such as the use of anti-virus technologies, fabricating or withholding personal information, and abstaining from some websites (e.g., Lee et al. 2008; Youn 2005; 2009). Accordingly, this study proposes that

H11: Young American consumers' perceived risk of online disclosure positively predicts their intent to (a) refuse information provision; (b) falsify personal information; (c) request the removal of personal information; (d) spread negative eWOM; (e) complain to online companies; and (f) report to the authorities.

Social Media Use and Privacy Protection

Heavy SNS users are more inclined to share personal information with friends, relatives, colleagues and acquaintances in social media to strengthen their social relationships. The growing literature on social media use contains a quite consistent finding that SNS are used to maintain offline relationships with friends, relatives, colleagues, and other acquaintances (Bolar 2009; Boyd and Ellison 2007; Chu and Choi 2010; Ray 2007). Heavy Internet and SNS users commonly have more offline social ties (Marshall et al. 2009; Zhao 2006).

In addition, frequent SNS visitors tend to have more trust in SNS as they believe that online companies and marketers have honored the implied social contract to protect their personal information. Accordingly, they feel more comfortable to disclose their personal information on SNS. Indeed, studies show that SNS users hold favorable attitudes toward SNS and have higher trust in SNS than non-users (Fogel and Nehmad 2009; Paek et al. 2011). It is reasonable to expect that the more time young American consumers spend on SNS, the less likely they will take action to protect online privacy. Hence, the following research hypothesis is proposed:

H12: Young American consumers' SNS use will negatively affect their online privacy protection intent to (a) refuse information provision; (b) falsify personal information; (c) request the removal of personal information; (d) spread negative eWOM; (e) complain to online companies; and (f) report to the authorities.

METHOD

An email containing a cover letter and a link to a web survey on Surveymonkey.com was sent to 2,500 randomly selected college students at a mid-sized public university in the southeastern United States in October, 2010. A college student sample is appropriate as well-educated young adults are more likely to use the Internet and social media (Lenhart et al. 2010; Rainie et al. 2003).

To boost the response rate, an incentive was conspicuously announced in the subject title of the email that one respondent would be randomly selected to receive a $100 online gift certificate and two respondents would receive a $50 certificate, both from Amazon.com. Cash and non-cash incentives can significantly increase the response rates of both mail surveys and Web-based surveys (Cobanoglu and Cobanoglu 2003; Dillman 2007).

The online survey consisted of a question about their use of SNS, a 4-item scale of Internet users' prior negative experience (Cho and Cheon 2004); Smith et al.'s (1996) 15-item scale of concerns for information privacy (CFIP); Merisavo et al.'s (2007) 3-item scale of Internet users' trust of online companies, marketers and laws; Malhotra et al.'s (2004) 5-item scale of perceived risk of online disclosure, six measures for behavioral intent to protect one's online privacy (Son and Kim 2008); and demographic questions. All measures are 5-point Likert scales except social media use measured at ratio level and demographic questions (see Appendix I). It took 10 days and three e-mailings to collect 403 completed usable questionnaires with no missing data.

With SPSS-19 and AMOS-19, the survey data set was analyzed using confirmatory factor analysis, principal axis factoring analysis, and structural equation modeling.

RESULTS

Four hundred three college students voluntarily participated in the web survey. The response rate was 16.1%. One hundred twenty-six respondents (31.3%) were male and 277 female (68.7%). The mean age of the sample was 21 (SD = 3.5), and respondents' ages ranged from 17-35. As for the typical daily use of SNS, respondents spent an average of 125.7 minutes on SNS (SD = 109.3, median = 120 minutes, mode = 60 minutes).

Table 1 presents Cronbach coefficients (α) of all adapted scales and the results of exploratory factor analyses (principle axis factoring with varimax rotation). A liberal minimum requirement for scale reliability is 0.60 (Churchill 1979; Peter 1979), while some scholars recommended a stricter minimum requirement of 0.70 (e.g., Nunnally and Bernstein 1994). Therefore, the performance of each of the four scales can be considered quite satisfactory. In addition, their extracted variances exceeded the 0.50 recommended level (Fornell and Larcker 1981).

TABLE 1

Scale Reliability and EFA Results

Construct	Mean	Cronbach α	Variance explained
Prior negative experience	3.05	.790	50.2%
CFIP	4.18	.889	60.6%
Perceived Trust	2.82	.744	52.8%
Perceived risk	3.56	.845	55.8%

Note. CFIP = Concern for Information Privacy. Variance Explained = Extraction sums of squared loadings of principal axis factoring. N = 403.

A confirmatory factor analysis also demonstrated that the CFIP measurement model performed very well on five important fitness indexes: $\chi^2 = 260.45$, $df = 87$, $p < .01$; Normed $\chi^2 = 2.99$; RMSEA = 0.070; TLI = 0.938; CFI = 0.948. They met four conventional standards very closely: the normed chi-square (the model chi-square divided by the degrees of freedom) in the 2:1 or 3:1 range (Carmines and McIver 1981), the Root Mean Square Error of Approximation (RMSEA) ≤ .06, Tucker-Lewis Index (TLI) ≥ .95, and Comparative Fit Index (CFI) ≥ .90 (Hu and Bentler 1999; Schumacker and Lomax 2004). Therefore, the CFIP model is considered a very parsimonious and satisfactory measure of young American Internet users' online privacy concerns, and is included in further analyses.

TABLE 2

Fit Indices for Six Research Models

Model	χ^2(df)	Normed χ^2	*RMSEA*	*TLI(NNFI)*	*CFI*
Research Model1	729.21 (355)*	2.05	0.051	0.924	0.934
Research Model2	743.34 (355)*	2.09	0.052	0.921	0.931
Research Model3	747.77 (355)*	2.11	0.052	0.921	0.931
Research Model4	734.20 (355)*	2.07	0.052	0.924	0.933
Research Model5	726.08 (355)*	2.05	0.051	0.925	0.934
Research Model6	720.10 (355)*	2.03	0.051	0.926	0.935

Note. RMSEA: root mean square error of approximation, GFI: goodness of fit index, TLI: the Tucker-Lewis index or NNFI: non-normed fit index, CFI: comparative fit index. * $p < .01$. $N = 403$.

The maximum likelihood method of structural equation modeling was adopted to fit the research model of Figure 1 to the survey data and test the hypotheses. Figures 2, 3, 4, 5, 6, and 7 present six tested structural models with standardized path estimates and critical ratios while Table 2 displays the model testing results.

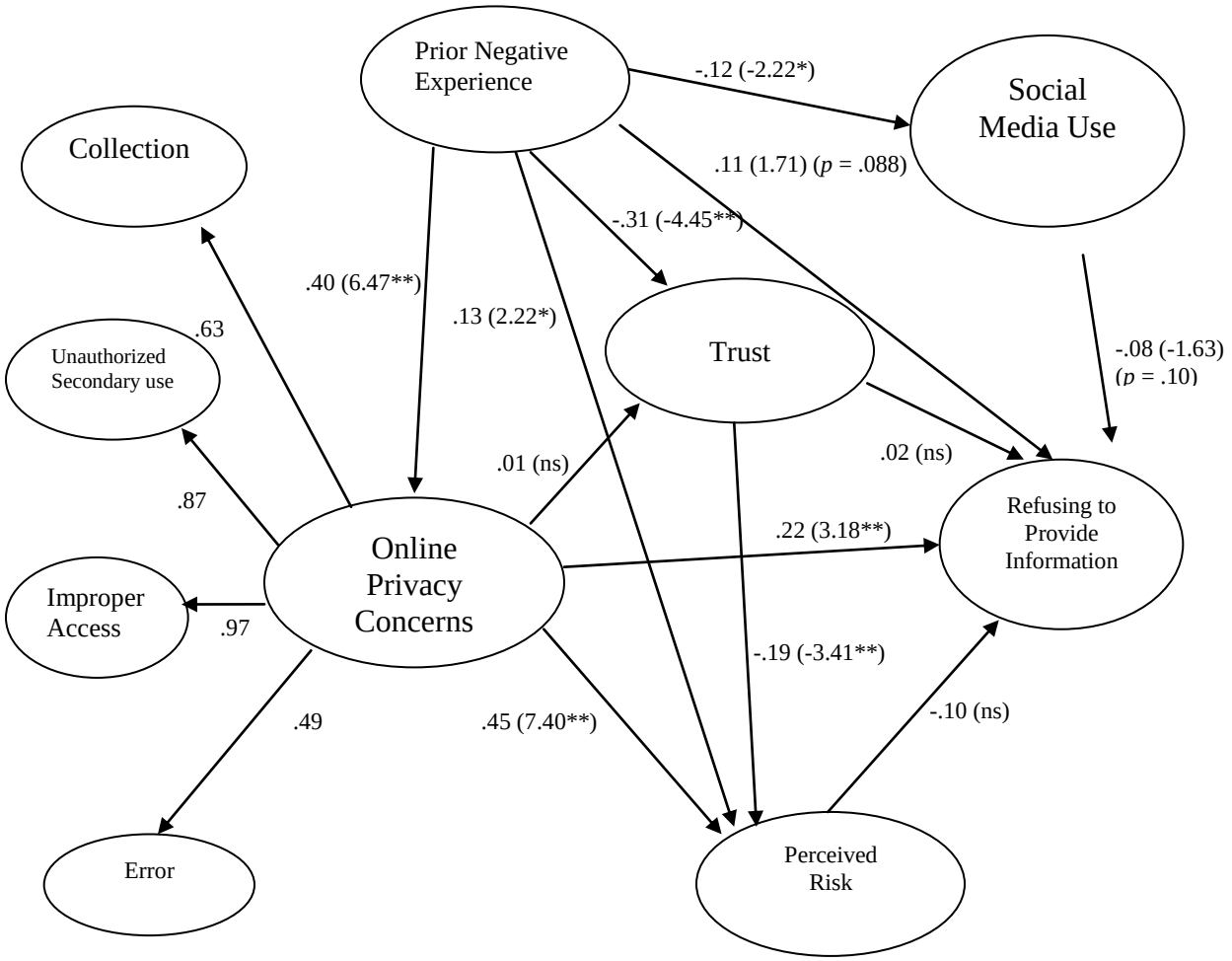
Six research models achieved satisfactory fit for young American consumers' behavioral intent to protect their online privacy. Six normed chi-square values were below 3:1 (Carmines and McIver 1981), six RMSEA values were smaller than the recommended cutoff value of .06 (Hu and Bentler 1999), and all comparative fit indices exceeded the conventional standard of .90 (Schumacker and Lomax 2004). Six Tucker-Lewis indexes were slightly below .95 probably because it penalized the complexity of the tested model. In addition, Marsh, Hau and Wen (2004) argue that the cutoff value of .95 for the TLI is probably too stringent for hypothesis testing. Therefore, the fitness of six models was deemed satisfactory.

The path estimates shown in Figures 2, 3, 4, 5, 6 and 7 supported Hypothesis 1. Young American consumers' prior negative experience of online disclosure strongly increased their online information privacy concerns. Similarly, H2 and H3 were confirmed. Students' bad past experience of online disclosure significantly heightened their risk perceptions of revealing personal information online while greatly undermined their trust in online companies, Internet marketers and laws to protect online privacy.

However, while H4b was strongly supported and H4a was marginally supported, H4c, H4d, H4e, and H4f were not supported. Young American consumers' prior negative experience positively predicted their intent to falsify personal information and refuse to provide personal information to some extent but did not directly influence their intent to request personal information removal, spread negative eWOM, complain to online companies, and report to the authority. On the other hand, H5 received sufficient empirical support. Unpleasant prior experience of online disclosure has a negative impact on their time spent on SNS.

FIGURE 2

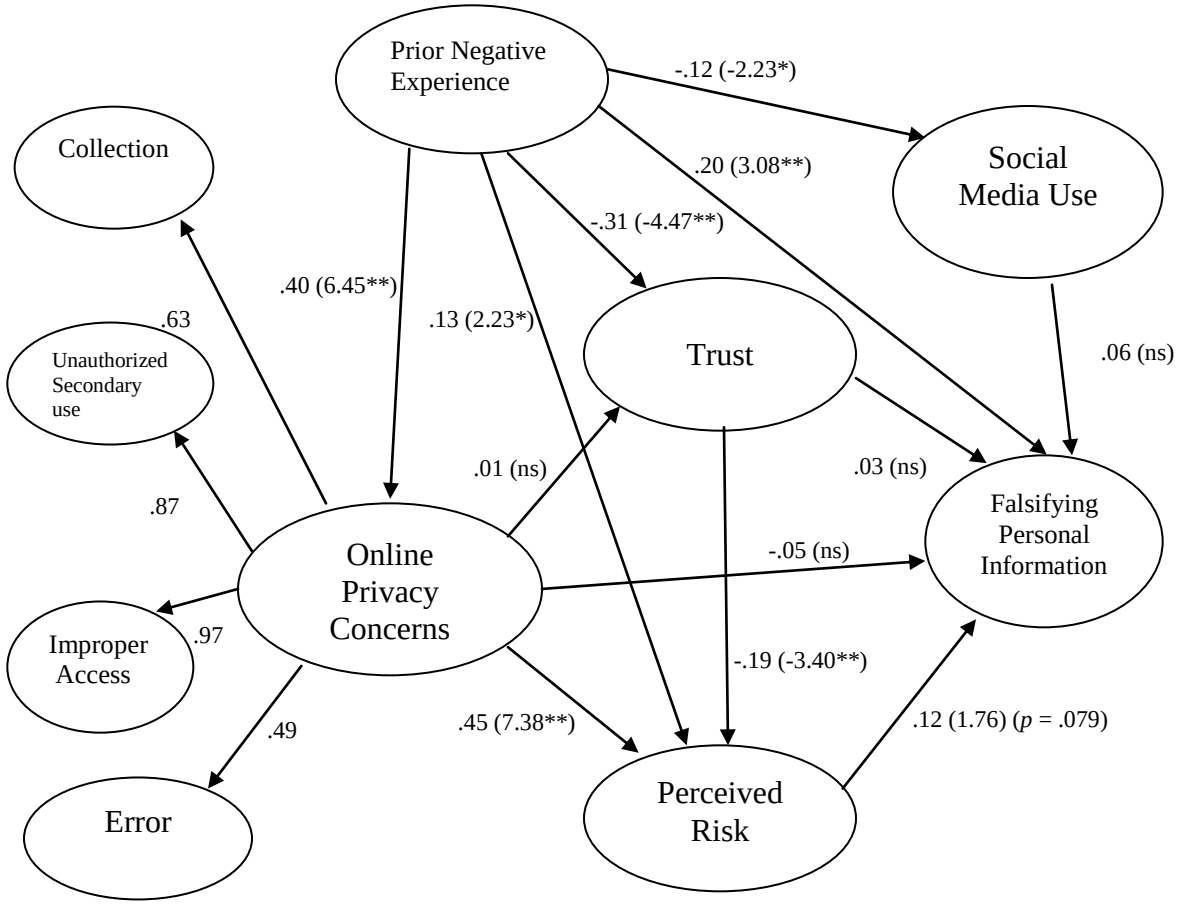
Structural Equation Model 1 with Standardized Path Estimates



Note. **Significance of the path estimates are shown in parentheses (critical ratio). *$p < .05$, **$p < .01$, ns = not significant. Model fit: $\chi^2 = 729.21$, $df = 355$, $p < .01$; RMSEA = 0.051; TLI = 0.924; CFI = 0.934. N = 403.**

FIGURE 3

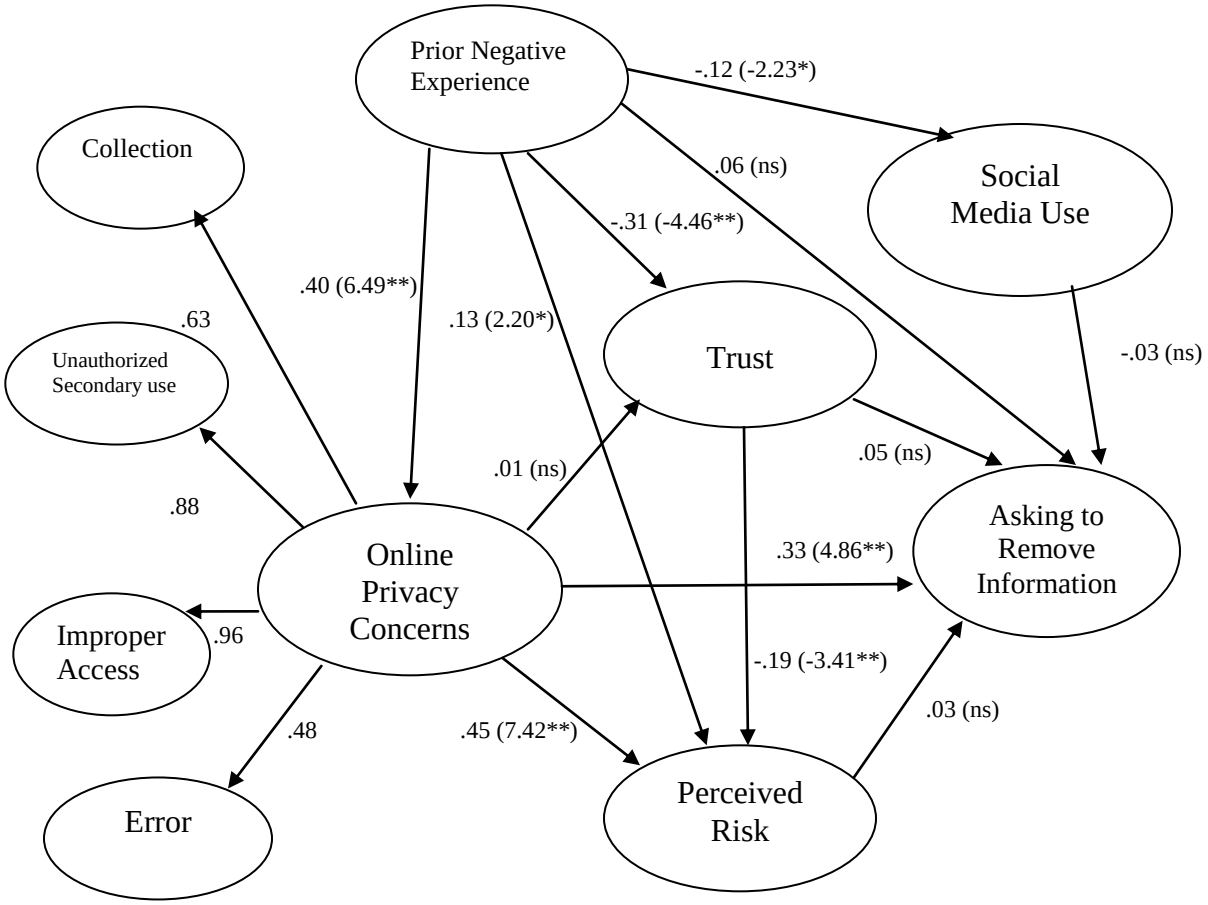
Structural Equation Model 2 with Standardized Path Estimates



Note. **Significance of the path estimates are shown in parentheses (critical ratio). *$p < .05$, **$p < .01$, ns = not significant. Model fit: $\chi^2 = 743.34$, $df = 355$, $p < .01$; RMSEA = 0.052; TLI = 0.921; CFI = 0.931. N = 403.**

FIGURE 4

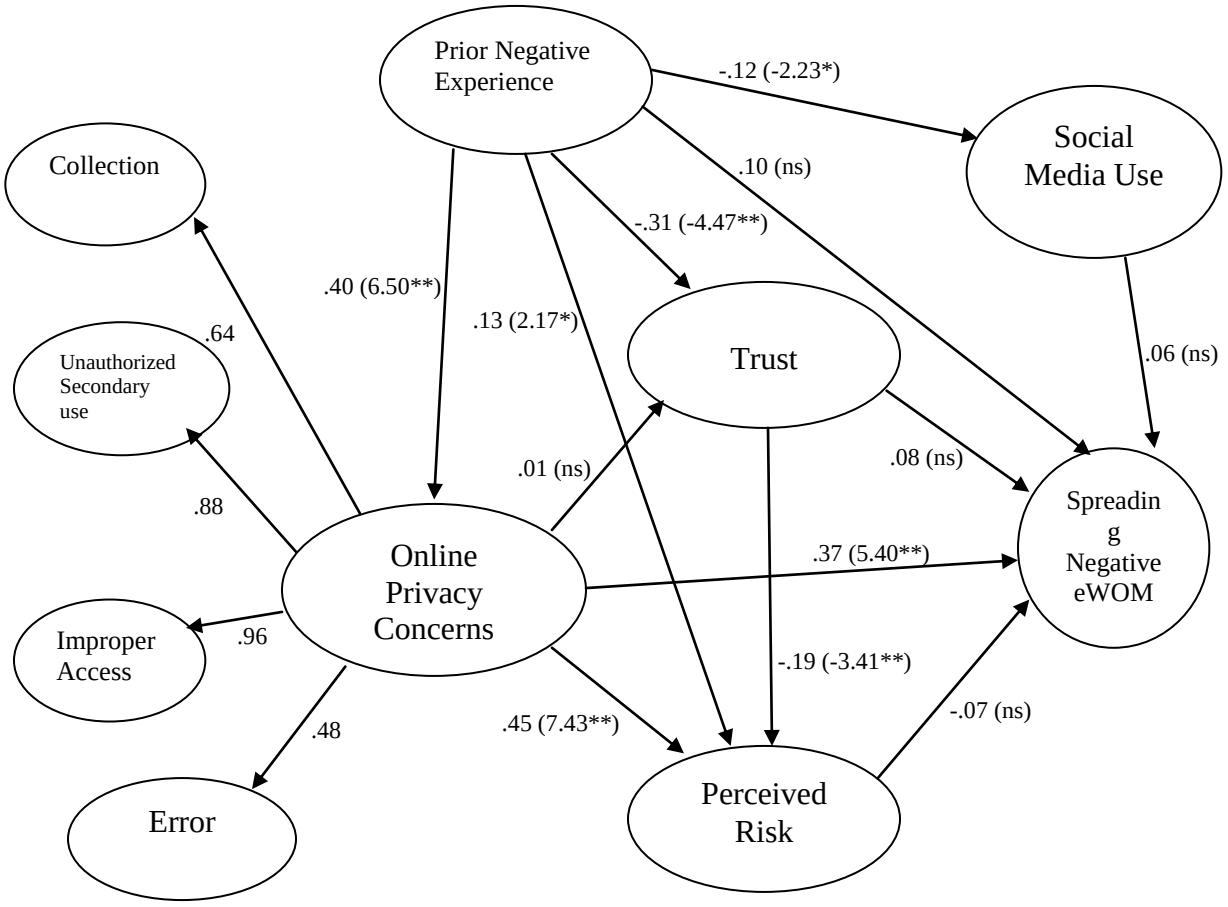
Structural Equation Model 3 with Standardized Path Estimates



Note. **Significance of the path estimates are shown in parentheses (critical ratio). *p < .05, **p < .01, ns = not significant. Model fit: χ^2 = 747.77, df = 355, p < .01; RMSEA = 0.052; TLI = 0.921; CFI = 0.931. N = 403**.

FIGURE 5

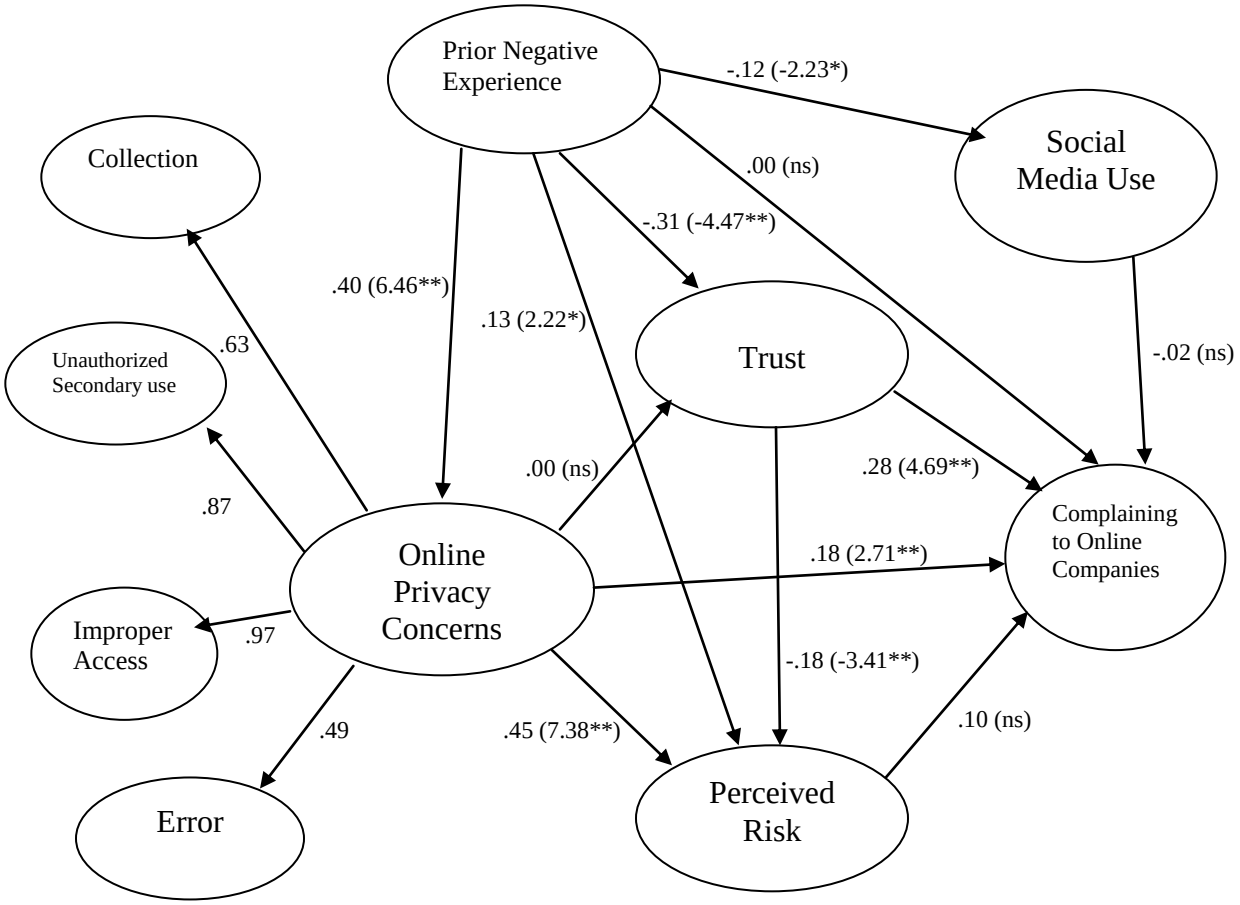
Structural Equation Model 4 with Standardized Path Estimates



Note. **Significance of the path estimates are shown in parentheses (critical ratio). *$p < .05$, **$p < .01$, ns = not significant. Model fit: $\chi^2 = 734.20$, $df = 355$, $p < .01$; RMSEA = 0.052; TLI = 0.924; CFI = 0.933. N = 403.**

FIGURE 6

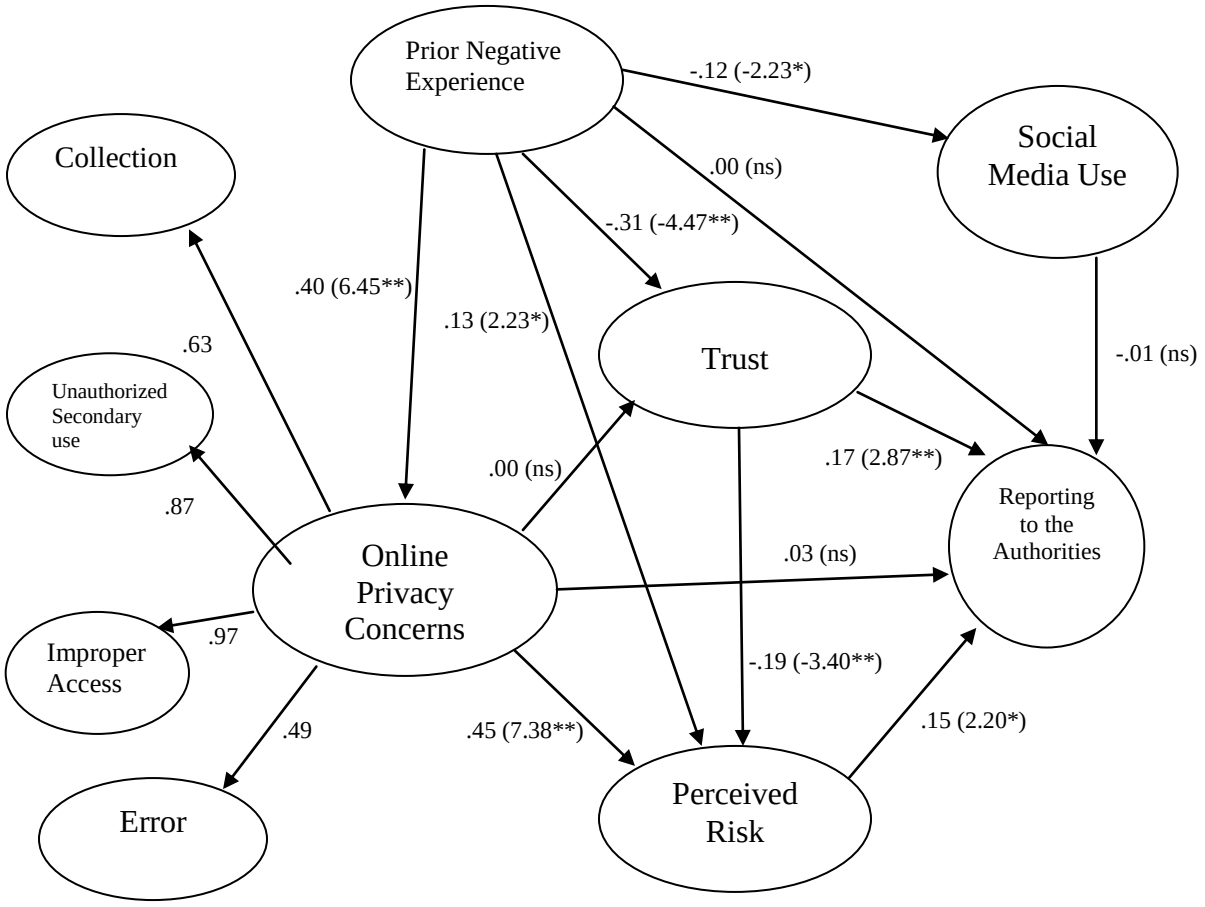
Structural Equation Model 5 with Standardized Path Estimates



Note. Significance of the path estimates are shown in parentheses (critical ratio). **p* < .05, ***p* < .01, ns = not significant. Model fit: χ^2 = 726.08, *df* = 355, *p* < .01; RMSEA = 0.051; TLI = 0.925; CFI = 0.934. N = 403.

FIGURE 7

Structural Equation Model 6 with Standardized Path Estimates



Note. **Significance of the path estimates are shown in parentheses (critical ratio). *$p < .05$, **$p < .01$, ns = not significant. Model fit: $\chi^2 = 720.10$, $df = 355$, $p < .01$; RMSEA = 0.051; TLI = 0.926; CFI = 0.935. N = 403.**

Surprisingly, Hypothesis 6 was not supported by any of the six tested models. Young American consumers' online privacy concerns did not mediate the effect of their prior negative experience of online disclosure on their trust in online companies, marketers and laws to protect online privacy. At the same time, their online privacy concerns greatly elevated their perceived risk of online disclosure, serving as a partial mediator of the effect of their prior negative experience of online disclosure on their perceived risk. Thus, Hypothesis 7 was strongly supported.

As shown in six significant, negative path estimates from trust to risk, young American consumers' trust in online companies, Internet marketers and laws to protect online privacy mitigated their perceived risk of online disclosure

considerably. Therefore, Hypothesis 8 was supported.

H9a, H9c, H9d, and H9e were supported but H9b and H9f were not confirmed. Young American consumers' online privacy concerns served as a good predictor of their online privacy protection intent to refuse information provision, request the removal of personal information, spread negative eWOM, and complain to online companies but had no direct effects on their intent to falsify personal information and report to the authority.

Unexpectedly, H10a, H10b, H10c, H10d, H10e, and H10f were not supported as young American consumers' trust in online companies, marketers and laws to protect online privacy did not negatively predict their intent to refuse information provision, falsify personal information, request the removal of personal information, and spread negative eWOM, but positively influenced their intent to complain to online companies and report to the authority.

As for H11f, it was supported while H11b arguably received marginal support. Young American consumers' perceived risk positively affected their intent to report to the authority and predicted their intent to falsify personal information online to some degree (p = 0.079). However, H11a, H11c, H11d, and H11e were not supported because perceived risk could not influence their intent to adopt other four privacy protection behaviors.

Finally, H12a received some marginal support but H12b, H12c, H12d, H12e, and H12f were all unsupported. Young American consumers' SNS use weakened their intent to refuse to provide personal information online to some extent. However, their SNS use did not negatively affect their intent to falsify personal information online, request the removal of personal information, spread negative eWOM, complain to online companies, and report to the authorities.

DISCUSSION AND IMPLICATIONS

Building upon previous published research and social contract theory, this study constructed and tested six research models of the impact of young American consumers' prior negative experience on their behavioral intent of online privacy protection through their online privacy concerns, trust, risk, and SNS use. Six causal models have achieved satisfactory fit. As one of the first studies, this empirical research has revealed how young consumers' online privacy concerns, trust, risk, and SNS use mediate the effects of their prior negative experience on their intent to adopt six privacy protection behaviors. The underlying dynamics provide useful insights for interactive marketing practitioners, policy makers and researchers.

Results of the present study suggest that interactive marketing managers must handle consumers' online personal data responsibly and sincerely address consumers' online privacy concerns so as to ensure the effectiveness of precise and targeted marketing in social media. As suggested by previous researchers (Lwin et al. 2007; Milne et al. 2004; Okazaki et al. 2009; Wirtz et al. 2007), Internet users believe that they have reached an implied social contract with social media companies when they volunteer their personal information on SNS and their online information privacy concerns will be greatly increased as soon as they discover that their online data are mishandled and their online privacy invaded. In turn, their risk perceptions of online disclosure will be greatly elevated. Their heightened online information privacy concerns will directly or indirectly drive them to take online privacy protective measures such as refusing to provide personal information, falsifying personal information, asking online companies to remove personal information, spreading negative eWOM about wrongdoers, complaining to online companies, and reporting to authority. As a result, social media marketing campaigns will become more and more irrelevant and impotent as most promotional messages are fed to social media users based on assumed truthful personal information they have disclosed.

Most importantly, this study has revealed that young American consumers' prior negative experience in online information disclosure greatly increases their online information privacy concerns, considerably heightens their risk perceptions of online disclosure, significantly undermines their trust in online companies, Internet marketers and laws to protect online privacy, evidently reduces their time spent on SNS, and positively predicts their intent to falsify personal information and refuse to provide personal information. These findings are generally consistent with previous studies (e.g., Bansal et al. 2010; Debatin et al. 2009; Goles et al.

2009; Okazaki et al. 2009; Pavlou and Gefen 2005; Sheehan and Hoy 1999; Son and Kim 2008). Apparently, the breach of an implied social contract by mishandling online information will immediately trigger young American consumers to take six privacy protective measures directly or indirectly by increasing their online privacy concerns or risk perceptions and reduce their time spent on SNS accordingly. In addition, their trust will be damaged and risk unmitigated.

SNS owners, operators and online marketers should use caution and care when monetizing subscribers' profiles by targeting ads to them or supplying their data to third parties. Once these subscribers perceive the abuse or misuse of their online privacy, they will probably refrain from and even discontinue using SNS. Frequent visitors to SNS will be a more valuable target audience to Internet marketers because they are more likely to reveal more personal identifying or lifestyle information or to notice or even to like a social ad or sponsored story. In this sense, SNS owners and operators should take customer relationship management very seriously and adopt proactive measures such as constant monitoring and addressing consumers' complaints about invasion of privacy responsively. These worried and dissatisfied users will not only turn into infrequent visitors but also refuse to provide their personal information, falsify their online personal data, ask you to remove their personal information, spread negative eWOM about you, and even report to the BBB or FTC in the near future if their online information concerns and/or risk perceptions are very high.

The study confirms that the 15-item CFIP scale of Smith et al. (1996) is likely a very good scale to measure American SNS users' information privacy concerns. This finding is not surprising as the CFIP scale has been validated in previous studies (e.g., Milberg, Smith, and Burke 2000; Rose 2006; Stewart and Segars 2002). It suggests that American SNS users are quite worried about collection of personal information, unauthorized secondary use, improper access to the collected online data or security, and inaccuracy of online personal database.

The results also demonstrate that young American consumers' online privacy concerns can directly increase their perceived risk of online information disclosure and affect their intent to refuse information provision, to request the removal of personal information, to spread negative eWOM and to complain to online companies. Their online privacy concerns fully and partially mediate the effects of their prior negative experience on their intent to take online privacy protection measures such as refusing to provide information online, asking for the removal of online data, spreading negative eWOM about perpetrators, and complaining to online companies.

Their online privacy concerns and trust mediate the effect of their prior negative experience of online disclosure on their intent to complain to online companies directly. Their trust and risk mediate the effect of their prior negative experience on their intent to report to the authority. Their online privacy concerns and trust partially mediate the effect of their prior negative experience on their perceived risk of online disclosure. The effect of their prior negative experience on their trust is not mediated by their online privacy concerns while trust can considerably alleviate perceived risk. Generally, these findings have validated previous studies of online privacy concerns, trust and risk (e.g., Jarvenpaa et al. 1999; McKnight et al. 2002; Malhotra et al. 2004; Pavlou 2003; Okazaki et al. 2009). They are also consistent with past research on online privacy concerns and self protection behaviors (e.g., Lwin et al. 2007; Milne et al. 2004; Moscardelli and Divine 2007; Sheehan and Hoy 1999; Wirtz et al. 2007; Youn 2009).

These findings have important implications for social media marketing. Both the industry and academia should be clearly aware that current young social media users are still very much concerned about their online privacy. If no proactive measure is adopted to address their online privacy concerns, they will be more likely to engage in online privacy protection behaviors such as refusing to provide personal information, requesting the removal of personal information, spreading negative eWOM and complaining to online companies. Online companies and marketers should improve their communication strategies to increase Internet users' awareness of their online information privacy policies and to minimize their online privacy concerns. Both advertising and public relations techniques should be utilized to build a trustworthy reputation in terms of online information privacy to minimize negative media coverage on SNS privacy issues. A responsive and proactive customer relationship management (CRM) team should be employed to

deal with any online privacy issues or controversies in a timely manner.

Unexpectedly, the study has found that Internet users' trust will positively influence their intent to complain to online companies and report to the authority. These findings hold a warning for online companies and marketers. Considering young American consumers' low initial trust (mean = 2.82 on a scale of 5), they should make extra efforts to gain it by taking some effective measures to address their high online privacy concerns, such as the open disclosure of one's online privacy policy (Miyazaki 2008) or seeking a privacy seal from BBBOnline or TRUSTe (Rifon et al. 2005). Otherwise, those SNS users with low initial trust could easily transform into bitter customers and citizens who will complain to one's customer service, and report privacy abuses and misuses to elected officials and consumer organizations.

Consumer advocacy groups and government agencies should be concerned that young American consumers' heightened risk does not motivate them to adopt five online privacy protection behaviors but online companies and Internet marketers should respect young American consumers' complaints to an elected official or consumer organization as their online privacy concerns and perceived risk are both severe when they choose to report privacy abuses to the authority. The results imply that, currently, young American consumers' perceived risk of online disclosure is not high enough to drive them to refuse to give personal information to online companies, to ask for personal information removal, to spread negative eWOM, and to complain to online companies directly but might drive some Internet users to falsify personal information online (p = .079). Indeed, respondents exhibited a moderate level of risk in disclosing personal information online. Therefore, it is still necessary to educate young Internet users about the risks of online over-disclosure and effective measures to protect their own online privacy.

On the other hand, the findings bode well for social media companies and Internet marketers. Young American consumers' perceived risk of online disclosure will probably stay so if social media companies and marketers conduct their business in good faith to honor the implied social contract. Until they have a negative experience of online privacy invasion, young Internet users likely will continue to take advantage of many benefits provided by SNS. Actually, a majority of the sample (63.4%) has not yet experienced an incident of online privacy invasion.

In addition, this research reveals that young American consumers' SNS use does not mediate the effects of their prior negative experience on their intent to adopt six online privacy protection measures even though the more time they spend on SNS, the more reluctant they will be to refuse to provide personal information to online companies. The results suggest that social media companies and Internet marketers should invest in customer relationship management and keep providing all users satisfactory services. Social media marketers should keep in mind that heavy SNS users or frequent SNS visitors do not necessarily let their guards down even though some of them will feel more uninhibited to provide their personal information to online companies. As heavy users or frequent visitors are more likely to reveal personal information online, it makes sense to target promotions to them and to encourage them to spread positive eWOM about a product or service. It is also advisable for social media marketers to ask frequent SNS users directly whether social ads are relevant to them while monitoring the click-through or "like" rate of these social ads or promotions.

Caution should be used when we generalize these findings to the general population due to some limitations. External validity should be strengthened by future researchers (the survey data in this study were collected from a random sample of college students at a single mid-sized Southeastern public university). Also, even if no gender difference was identified in key variables, research findings are skewed slightly as the majority of participants (69%) were female.

Finally, future research should investigate other antecedents and consequences of SNS users' online privacy protection behaviors, including need for privacy, self-efficacy, subjective norm, behavioral control, perceived benefits of online disclosure, willingness to provide information online, and regulatory support. Future studies should also explore these topics in a cross-cultural and global context.

CONCLUSION

After successfully testing six research models of the effects of young American consumers' prior negative experience on their intent to adopt six privacy protection behaviors through their online privacy concerns, trust, risk, and SNS use: the present study shows that young American consumers' prior negative experience in online information disclosure directly increases their online information privacy concerns; heightens their risk perceptions of online disclosure; undermines their trust in online companies, Internet marketers and laws to protect online privacy; reduces their time spent on SNS; and enhances their intent to falsify personal information and/or refuse to provide personal information.

Young American consumers' online privacy concerns can also elevate their perceived risk of online information disclosure and strengthen their intent to refuse information provision, to request the removal of personal information, to spread negative eWOM and to complain to online companies. Their online privacy concerns about trust and risk work together to mediate the effects of their prior negative experience on their intent to take online privacy measures such as complaining to online companies and reporting to the author.

Young American Internet users are highly concerned about collection of personal information, unauthorized secondary use, improper access to the collected online data or security, and inaccuracy of online personal databases.

Their SNS use does not mediate the effects of their prior negative experience on their intent to adopt six online privacy protection measures but might predict some heavy users' willingness to provide more personal information online.

REFERENCES

Acquisti, Alessandro, and Ralph Gross (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK.

Awad, Naveen Farag, and M.S. Krishnan (2006), "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly*, 30(1): 13–28.

Bansal, Gaurav, Fatemeh "Mariam" Zahedi, and David Gefen (2010), "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, 49(2), 138-50.

Bolar, Kartikeya P. (2009), "Motives Behind the Use of Social Networking Sites: An Empirical Study," *ICFAI Journal of Management Research*, 8(1), 75-84.

Boyd, Danah M. and Nicole B. Ellison (2007), "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication*, 13(1) (accessed 9/23/11), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Carmines Edward G. and John P. McIver (1981), "Analyzing Models with Unobserved Variables: Analysis of Covariance Structures," In *Social Measurement: Current Issues*, George W. Bohrnstedt and Edgar F. Borgatta, eds, Beverly Hills, CA: Sage Publications, 65-115.

Cases, Anne-Sophie (2002), "Perceived risk and risk-reduction in Internet shopping," *The International Review of Retail, Distribution and Consumer Research*, 12 (4), 375-394.

Chen, Xi, and Shi, Shuo (2009), "A Literature Review of Privacy Research on Social Network Sites," In *the Proceedings of the First International Conference on Multimedia Information Networking and Security*, Los Alamitos, CA: IEEE Computer Society, 93-97.

Cho, Chang-Hoan and Hongsik John Cheon (2004), "Why do people avoid advertising on the Internet?," *Journal of Advertising*, 33 (4), 89-97.

Chu, Shu-Chuan and Sejung Marina Choi (2010), "Social capital and self-presentation on social networking sites: a comparative study of Chinese and American young generations," *Chinese Journal of Communication*, 3(4), 402-420.

Churchill, Gilbert A. Jr. (1979), "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research*, 16(1), 64-73.

Cobanoglu, Cihan, and Nesrin Cobanoglu (2003), "The effect of incentives in web surveys: Application and ethical considerations," *International Journal of Market Research*, 45(4), 475-488.

Comegys, Charles, Mika Hannula, and Jaani Väisänen (2009), "Effects of Consumer Trust and Risk on Online Purchase Decision-making: A Comparison of Finnish and United States Students," *International Journal of Management*, 26(2), 295-308.

Culnan, Mary J. (1993), "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly*, 17 (3), 341-63.

Culnan, Mary J. (1995), "Consumer awareness of name removal procedures: Implications for direct marketing," *Journal of Direct Marketing*, 9(2), 10-19.

Culnan, Mary J., and Pamela K. Armstrong (1999), "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, 10 (1), 104-115.

Culnan, Mary J. and Robert J. Bies (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, 59 (2), 323-42.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15, 83-108.

Dillman, Don A. (2007), *Mail and internet surveys: The tailored design method*, Hoboken, N.J: Wiley.

Dvorak, John C. (2010), "Why Facebook privacy settings don't matter," *PC Magazine*, 29(7), 1.

Ellison, Nicole B., Charles Steinfield, and Cliff Lampe (2007), "The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication*, 12 (4), 1143-68.

eMarketer Inc. (2012a), "Google Edges Closer to Facebook as US Display Advertising Becomes Two-Horse Race," www.emarketer.com/PressRelease.aspx?R=1008856 (accessed August 5, 2012).

eMarketer Inc. (2012b), "Total Worldwide Social Network Ad Revenues Continue Strong Growth," www.emarketer.com/Article.aspx?R=1008862 (accessed August 5, 2012).

Federal Trade Commission (FTC) (1998), *Privacy Online: A Report to Congress*, (June), Washington, DC: Federal Trade Commission.

Federal Trade Commission (FTC) (2010), *FTC Testifies on Do Not Track Legislation*, www.ftc.gov/opa/2010/12/dnttestimony.shtm (accessed September 25, 2011)

Fogel, Joshua and Elham Nehmad (2009), "Internet social network communities: Risk taking, trust, and privacy concerns," *Computers in Human Behavior*, 25 (1), 153-60.

Fornell, Claes and David F. Larcker (1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, 18 (1), 39-50.

Fox, Susannah (2000), *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, www.pewinternet.org/~/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf (accessed September 28, 2011)

Goles, Tim, Simon Lee, Srinivasan V. Rao, and John Warren (2009), "Trust Violation in Electronic Commerce: Customer Concerns and Reactions," *The Journal of Computer Information Systems*, 49(4): 1-9.

Gross, Ralph, and Alessandro Acquisti (2005, November). *Information revelation and privacy in online social networks*. Paper presented at the ACM Workshop on Privacy in the Electronic Society, Alexandria, VA.

Hof, Robert D. (2011), "Facebook's new ad model: You," *Forbes*, 188(10) 106-110.

Holson, Laura M., and Miguel Helft (2010), "Going private," *New York Times Upfront*, 143(2), September 20, 14-15.

Hoofnagle, Chris Jay, Jennifer King, Su Li, and Joseph Turow (2010), "How different are young adults from older adults when it comes to information privacy attitudes and policies?" Faculty Working Paper, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 (accessed November 4, 2011).

Hoy, Mariea Grubbs, and George Milne (2010), "Gender Difference in Privacy-Related measures for Young Adult Facebook Users," *Journal of Interactive Advertising*, 10(2), 28-45.

Hu, Li-tze, and Peter M. Bentler (1999), "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling*, 6(1), 1-55.

Janda, Swinder, and Lindsey L. Fair (2004), "Exploring consumer concerns related to the Internet," *Journal of Internet Commerce*, 3 (1), 1-21.

Jarvenpaa, Sirkka L., Noam Tractinsky, Lauri Saarinen, and Michael Vitale (1999), "Consumer trust in an internet store: A cross-cultural validation," *Journal of Computer-mediated Communication*, 5(2), http://jcmc.indiana.edu/vol5/issue2/jarvenpaa.html (accessed September 30, 2011)

Jones, Harvey and José Hiram Soltren (2005), "Facebook: Threats to Privacy," http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (accessed September 24, 2011)

Joinson, Adam N., Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield (2010), "Privacy, Trust, and Self-Disclosure Online," *Human-Computer Interaction*, 25(1), 1-24.

Khang, Hyoungkoo, Eyun-Jung Ki, and Lan Ye (2012), "Social Media Research in Advertising, Communication, Marketing, and Public Relations, 1997-2010," *Journalism & Mass Communication Quarterly*, 89(2), 279-298.

Larose, Robert and Nora J. Rifon (2007), "Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior," *Journal of Consumer Affairs*, 41 (1), 127-49.

Learmonth, Michael (2010), "Facebook Stirs up Trouble for Valley," *Advertising Age*, 81(18), 1 & 117.

Lee, Doohwang, Robert LaRose, and Nora Rifon (2008), "Keeping Our Network Safe: A Model of Online Protection Behavior," *Behaviour & Information Technology*, 27(5), 445–454

Lenhart, Amanda, Kristen Purcell, Aaron Smith, and Kathryn Zickuhr (2010), "Social Media and Young Adults, *PewInternet and American Life Project*, www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx (accessed September 24, 2011).

Lwin, May, Jochen Wirtz, and Jerome D. Williams (2007), "Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective," *Journal of the Academy of Marketing Science*, 35 (4), 572-85.

Madden, Mary, and Aaron Smith (2010), *Reputation management and social media: How people monitor their Internet identity and search for othersonline*, www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf (accessed November 4, 2011).

Malhotra, Naresh K., S. Kim Sung, and James Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, 15 (4), 336-55.

Marsh, Herbert W., Kit-Tai Hau, and Zhonglin Wen (2004), "In Search of Golden Rules: Comment on Hypothesis-Testing Approaches to Setting Cutoff Values for Fit Indexes and Dangers in Overgeneralizing Hu and Bentler's (1999) Findings," *Structural Equation Modeling*, 11 (3), 320-41.

Marshall, Bryan, Jeongil Choi, Maha M. El-Shinnaway, Matthew North, Lars Svensson, Sujie Wang, Daniel T. Norris, Lixin Cui, Natalya Goreva, Voraphan Raungpaka, Ayseli Usluata, Catherine Whelan, Juyun Cho, Caroline Collier, Stefan Nillson, Gilard Ravid and Juan Pablo Valenzuala (2009), "Online and Offline Social Ties of Social Network Website Users: An Exploratory Study in Eleven Societies," *Journal of Computer Information Systems*, 50 (1): 54-64.

McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar (2002), "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research*, 13 (3), 334-59.

Merisavo, Marko, Sami Kajalo, Heikki Karjaluoto, Ville Virtanen, Sami Salmenkivi, Mika Raulas, and Matti Leppäniemi (2007), "An Empirical Study of the Drivers of Consumer Acceptance of Mobile Advertising," *Journal of Interactive Advertising*, 7(2), 1-17.

Metzger, Miriam J. (2004), "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication*,9(4), http://jcmc.indiana.edu/vol9/issue4/metzger.html (accessed September 27, 2011)

Metzger, Miriam J. (2006), "Effects of site, vendor, and consumer characteristics on website trust and disclosure," *Communication Research*, 33 (3), 155-179.

Metzger, Miriam J. and Sharon Docter (2003), "Public Opinion and Policy Initiatives for Online Privacy Protection," *Journal of Broadcasting & Electronic Media*, 47 (3), 350-74.

Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke (2000), "Information Privacy: Corporate Management and National Regulation," *Organization Science*, 11 (1), 35-57.

Milne, George R. (1997), "Consumer Participation in Mailing Lists: A Field Experiment," *Journal of Public Policy & Marketing,* 16(2), 298-309.

Milne, George R., and Mary Ellen Gordon (1993), "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework," *Journal of Public Policy & Marketing*, 12(2), 206-215.

Milne, George R., Andrew J. Rohm, and Shalini Bahl (2004), "Consumers' Protection of Online Privacy and Identity," *The Journal of Consumer Affairs*, 38(2), 217–232.

Miyazaki, Anthony D. (2008), "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," *Journal of Public Policy & Marketing*, 27 (1), 19-33.

Miyazaki, Anthony D. and Ana Fernandez (2001), "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *Journal of Consumer Affairs*, 35 (1), 27-44.

Moscardelli, Deborah M., and Richard Divine (2007), "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), 232-252.

Myerscough, Stuart, Ben Lowe, and Frank Alpert (2006), "Willingness to Provide Personal Information Online: The Role of Perceived Privacy Risk, Privacy Statements and Brand Strength," *Journal of Website Promotion*, 2(1/2), 115-140.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs*, 41, (1), 100-126.

Nunnally, Jum C., and Ira H. Bernstein (1994), *Psychometric theory*, New York: McGraw-Hill, Inc.

O'Brien, Kevin (2010), "Despite privacy inquiries, Germans flock to Google, Facebook and Apple," *New York Times*, July 12, 8.

Okazaki, Shintaro, Hairong Li, and Morikazu Hirose (2009), "Consumer privacy concerns and preference for degree of regulatory control," *Journal of Advertising*, 38 (4), 63-77.

Olivero, Nadia and Peter Lunt (2004), "Privacy versus Willingness to Disclose in E-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control," *Journal of Economic Psychology*, 25 (2), 243-62.

Paek, Hye-Jin, Beom Jun Bae, Thomas Hove, and Hyunjae Yu (2011), "The perceived benefits of six-degree-separation social networks," *Internet Research*, 21(1), 26-45.

Pavlou, Paul A. (2003), "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*, 7 (3), 101-34.

Pavlou, Paul A. and David Gefen (2005), "Psychological contract violation in online marketplaces: antecedents, consequences, and moderating role," *Information Systems Research*, 16(4): 372–434.

Peter, J. Paul (1979), "Reliability: A Review of Psychometric Basics and Recent Marketing Practices," *Journal of Marketing Research*, 16(1), 6-17.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell (2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, 19(1), 27-41.

Quinn, James (2010, August 5), "Facebook Clicks with Advertisers," *The Daily Telegraph*, p. 3.

Rainie, Lee, Mary Madden, Angie Boyce, Amanda Lenhart, John Horrigan, Katherine Allen, and Erin O'Grady (2003), "The Ever-Shifting Internet Population: A new look at Internet access and the digital divide," *Pew Internet and American Life Project*, www.pewinternet.org/Reports/2003/The-EverShifting-Internet-Population-A-new-look-at-Internet-access-and-the-digital-divide.aspx (accessed September 24, 2011).

Ray, Mary Beth (2007), "Needs, Motives, and Behaviors in Computer-Mediated Communication: An Inductive Exploration of Social Networking Websites," Paper presented at International Communication Association Conference, San Francisco, CA.

Rifon, Nora J., Robert LaRose, and Sejung Marina Choi (2005), "Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures," *Journal of Consumer Affairs*, 39(2), 339-362.

Rogers, Ronald W. (1975), "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology*, 91 (1), 93–114.

Rose, Ellen A. (2006), "An examination of the concern for information privacy in the New Zealand regulatory context," *Information & Management*, 43(3), 322-335.

Schumacker, Randall E. and Richard G. Lomax (2004), *A beginner's guide to structural equation modeling (Second Edition)*, Mahwah, NJ: Lawrence Erlbaum Associates.

Sheehan, Kim Bartel and Marlea Grubbs Hoy (1999), "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns," *Journal of Advertising*, 28(3), 37-51.

Sheehan, Kim Bartel and Mariea Grubbs Hoy (2000), "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, 19(1), 62-73.

Shin, Dong-Hee (2010), "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), 428-438.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, 20(2), 167–196.

Son, Jai-Yeol and Sung S. Kim (2008), "Internet users' information privacy protective response: a taxonomy and a nomological model," *MIS Quarterly*, 32(3), 503-529.

Stewart, Kathy A. and Albert H. Segars (2002), "An empirical examination of the concern for information privacy instrument," *Information Systems Research*, 13(1), 36–49.

Stutzman, Fred (2006), "An Evaluation of Identity-Sharing Behavior in Social Network Communities," *International Digital and Media Arts Journal*, 3(1), www.units.muohio.edu/codeconference/papers/papers/stutzman_track5.pdf (accessed September 28, 2011)

Terlep, Sharon, Suzanne Vranica, and Shayndi Raice (2012), "GM Says Facebook Ads Don't Pay Off," *Wall Street Journal - Eastern Edition*, May 16. A1.

Wirtz, Jochen, May O. Lwin, and Jerome D. Williams (2007), "Causes and consequences of consumer online privacy concern," *International Journal of Service Industry Management*, 18(4), 326-348.

Youn, Seounmi (2005), "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *Journal of Broadcasting & Electronic Media*, 49 (1), 86–110.

Youn, Seounmi (2009), "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents," *Journal of Consumer Affairs*, 43(3), 389-418.

Zhao, Shanyang (2006), "Do Internet users have more social ties? A call for differentiated analyses of Internet use," *Journal of Computer-Mediated Communication*, 11, 844-862.

Send correspondence regarding this article to :

Hongwei (Chris) Yang, Ph.D.
Assistant Professor
Department of Communication
Appalachian State University
ASU Box 32039
Boone, NC 28608-2039
Tel: 828-262-6972
Fax: 828-262-2543
yangh@appstate.edu

APPENDIX I

The Primary Survey Questions

Social Media Use	Two open ended questions 1. How much time do you spend on social networking websites (e.g., Facebook, MySpace, LinkedIn, Classmates, etc) on a typical day? **2.** How much time do you spend on blogging websites (e.g., Twitter, Wordpress, Blogger, etc) on a typical day?
Prior negative experience*[1]	1. I have seen my personal information misused by companies without my authorization. 2. I feel dissatisfied with my earlier choice to provide my personal information to Internet marketers. 3. My experience in responding to Internet advertising is very unsatisfactory. 4. In the past, my decision to provide my personal information to Internet marketers has not been a wise one.
Concern for Information Privacy*[2]	Collection 1. It usually bothers me when online companies ask me for personal information. 2. When online companies ask me for personal information, I sometimes think twice before providing it. 3. It bothers me to give personal information to so many online companies. 4. I'm concerned that online companies are collecting too much personal information about me. Unauthorized secondary use 1. Online companies should not use personal information for any purpose unless it has been authorized by the individuals who provided information. 2. When people give personal information to an online company for some reason, the online company should never use the information for any other reason. 3. Online companies should never sell the personal information in their computer databases to other companies. 4. Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information. Improper access 1. Online companies should devote more time and effort to preventing unauthorized access to personal information. 2. Online companies' computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs. 3. Online companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

	Error 1. Online companies should take more steps to make sure that the personal information in their files is accurate. 2. Online companies should have better procedures to correct errors in consumers' personal information. 3. Online companies should devote more time and effort to verifying the accuracy of the personal information in their databases. 4. All the personal information in online companies' computer databases should be double-checked for accuracy—no matter how much this costs.
Internet users' perceived risk*[3]	1. In general, it would be risky to give (the information) to online companies. 2. There would be high potential for loss associated with giving (the information) to online firms. 3. There would be too much uncertainty associated with giving (the information) to online firms. 4. Providing online firms with (the information) would involve many unexpected problems. 5. I would feel safe giving (the information) to online companies (reverse).
Trust in privacy and laws of Internet advertising*[4]	1. I believe that my Internet service provider uses my data only for a purpose that I have approved. 2. I believe that an Internet marketer would use my data only for a purpose that I have approved. **3.** I believe that consumers' online data privacy is protected by laws.
Internet users' intents to protect online privacy[5]	1. How likely would you refuse to give information to online companies when you think it is too personal within the next six months? 2. How likely would you falsify some of your personal information when asked by online companies within the next six months? 3. How likely would you take actions to have your information removed from online companies' database when your personal information was not properly handled? 4. How likely would you speak to your friends and/or relatives about your bad experience with online companies' mishandling personal information when your personal information was not properly handled? 5. How likely would you write or call online companies to complain about the way they use personal information when your personal information was not properly handled? **6.** How likely would you write or call an elected official or consumer organization to complain about the way online companies use personal information when your personal information was not properly handled?

*The response options ranged from 1, "strongly disagree" to 5, "strongly agree"
*[1]Adapted from Cho & Cheon (2004). *[2] Adapted from Smith et al. (1996). *[3]Adapted from Malhotra, Kim, and Agarwal (2004). *[4]Adapted from Merisavo et al. (2007). [5]Adapted from Son and Kim (2008), anchored by 1, "very unlikely" to 5, "very likely."