CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING
Volume 18, Number 1, 2015

DOI: 10.1089/cyber.2014.0456

Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection

Hsuan-Ting Chen, PhD,[1] and Wenhong Chen, PhD[2]

Abstract

Sampling 515 college students, this study investigates how privacy protection, including profile visibility, self-disclosure, and friending, are influenced by privacy concerns and efficacy regarding one's own ability to manage privacy settings, a factor that researchers have yet to give a great deal of attention to in the context of social networking sites (SNSs). The results of this study indicate an inconsistency in adopting strategies to protect privacy, a disconnect from limiting profile visibility and friending to self-disclosure. More specifically, privacy concerns lead SNS users to limit their profile visibility and discourage them from expanding their network. However, they do not constrain self-disclosure. Similarly, while self-efficacy in privacy management encourages SNS users to limit their profile visibility, it facilitates self-disclosure. This suggests that if users are limiting their profile visibility and constraining their friending behaviors, it does not necessarily mean they will reduce self-disclosure on SNSs because these behaviors are predicted by different factors. In addition, the study finds an interaction effect between privacy concerns and self-efficacy in privacy management on friending. It points to the potential problem of increased risk-taking behaviors resulting from high self-efficacy in privacy management and low privacy concerns.

Introduction

SOCIAL NETWORKING SITES (SNSs)—defined "as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system (p. 211)"[1]—have brought growing attention to the issue of privacy due to their rapid expansion and interweaving into individuals' daily lives.[1–4] Jealous romantic partners and watchful employers are not the only ones scrutizing users' profiles and status udpates. Various third parties, such as advertisers, app developers, insurance providers, and academic researchers, mine user data for information. One's reputation and career may also be haunted by imprudent sharing on SNSs.[5,6]

Although the potential threats to privacy are high on SNSs, studies have produced mixed results regarding the relationships between privacy concerns, SNS usage, and privacy-protecting behaviors.[7] When it comes to using SNSs, individuals are not always constrained by privacy concerns. In fact, privacy concerns have little impact on SNS usage behaviors when the observed risks of disclosing personal data are outweighed by the perceived benefits of online social networking, such as popularity, identity construction, network expanding, relationship maintenance, and self-presentation.[3,7,8]

This study focuses on privacy on Facebook given its dominant status among SNSs, its requirement of using real user information, as well as its controversial track record in protecting user privacy. For instance, different from online chatrooms or forums in the early days of Internet diffusion, nonymity replaces anonymity on Facebook, as users are asked to use real personal information, which affects the presentation of self, as users are connecting to their offline network in their daily lives.[9] In addition, Facebook has continually changed what personal information is visible, such as basic demographic background, wall posts, photos, friends, networks, and likes, and how this personal information is classified.[5]

This study examines privacy on Facebook by not only investigating privacy concerns but also exploring the role of self-efficacy in privacy management—the extent to which users are confident in their ability to manage privacy settings—to understand their relationships with privacy protection on SNSs. Self-efficacy in privacy management, which has yet to receive

[1]School of Journalism and Communication, The Chinese University of Hong Kong, Shatin, Hong Kong.
[2]Department of Radio-TV-Film, The University of Texas at Austin, Austin, Texas.

sufficient attention in research on SNS privacy, may help to explain why SNS users voicing their concern about privacy still behave as if unconcerned. SNS users who are confident in themselves as highly capable of managing privacy settings may have privacy risk-taking behavior on SNSs.

This study examines how individuals' privacy concerns and self-efficacy in privacy management are related to privacy protection. This study adopts Ellison et al.'s three privacy protecting strategies by which users can control the audience for their disclosures on SNSs: limiting their profile visibility, self-disclosure, and friending.[10] This study also explores the interaction relationship between privacy concerns and self-efficacy in privacy management given that a person's self-efficacy in how well he or she can manage privacy settings may play a moderating role in influencing the relationship between privacy concerns and privacy protection.

Privacy on SNSs

It is important to understand the concept of privacy to provide a conceptual foundation about how the concept has evolved in the new communication environment, and how it is applied in the context of SNSs. The concept of privacy as a legal right in the modern sense originates from Warren and Brandeis, who said the spirit of privacy is ''the right to be let alone (p.193).''[11] The rise of the Internet facilitates the development of an active approach to protecting privacy, which is empowering individuals to protect themselves instead of simply allowing them to be passively let alone. Privacy is taking control over information about ourselves.[12] Individuals have greater responsibility than they had before to decide to what extent they would like to share their personal information. Westin defined information privacy as ''the claim of individuals, groups, or institutions to determine themselves when, how, and to what extent information about them is communicated to others (p.7).''[13] This concept is closely related to information and communication technologies, and it has been applied to research on SNS privacy.[14,15]

Although the concept of privacy has evolved from the right to be left alone to the right to control personal information, there has been an increase in publicly displaying one's personal information and network on SNSs. SNSs often require users to use real names and share personally identifiable, authentic, and accurate information.[16] Sharing is built in and encouraged through system design in SNSs. Although SNSs such as Facebook claim that using and sharing real information can create more engaging and meaningful experiences, more sharing also leads to large-scale data collection.[9] Facebook can share those in-depth characteristics and personal information with advertisers and other third parties. Even though the privacy concern on SNSs is high, it was not until the beginning of 2008 that Facebook implemented a privacy setting function. However, the Federal Trade Commission found that Facebook misled users about how their data were shared.[17] In addition, SNS users trade their privacy for benefits on SNSs such as social rewards, popularity, and enjoyment as they disclose personal information.[7,8,18] Therefore, the important questions to examine are what factors may enhance privacy protection on SNSs and what factors may mitigate it to understand the privacy trade-off.

Privacy calculus model

The privacy calculus model proposes that contrary beliefs act as situational contracts in affecting behavior simultaneously.[14] Extending from the typical behavioral models such as the theory of planned behavior that examines the influence of noncontrary beliefs on behavior,[19] the privacy calculus model has been applied in different areas, such as e-commerce, Internet use, and job hunting to examine the factors that simultaneously influence users' information disclosure and privacy protection.[14,20–22] For example, when privacy concerns curb self-disclosure, entertainment, trust in service providers, relationship maintenance, and other benefits motivate people to reveal personal information.[23,24] As Culnan and Bies argued, ''a positive net outcome should mean that people are more likely to accept the loss of privacy that accompanies any disclosure of personal information as long as an acceptable level of risk accompanies the benefits (p.327).''[25] To disclose personal information or not depends on an assessment of the costs and benefits. This model can therefore help illuminate the privacy paradox on SNSs that individuals concerned about privacy do not necessarily act to protect their privacy; instead, they may reveal a large amount of personal information.[2,3,26]

Privacy concerns and privacy protection

Privacy concerns are examined as a risk belief, which is a cost, in the privacy calculus model.[14,15,24,27] They are positively related to privacy protection, as those who are concerned about their online privacy tend to adopt behaviors controlling their information disclosure and reducing online risks from privacy invasion.[28–32] More recently, the model has been applied to the context of SNSs.[24,33] To protect privacy on SNSs, users can adopt strategies to control what information they would like to disclose and share and with whom, including adjusting their profile visibility, friending, and self-disclosure.[10] For example, SNS users can make a public profile into a private profile, so their personal information can only be accessed by certain groups of people. In addition, they can restrict access to shared information such as wall posts, status updates, tagging, photos, and videos to a select number of friends.[34] SNS users can also reduce the personal information they disclose as a strategy to control their information. Thus, those who have high privacy concerns should tend to limit their profile visibility and reduce their self-disclosure. They would also be less likely to expand their social network to protect their privacy and minimize the privacy risk.

H1: The level of privacy concerns is positively related to limiting profile visibility.

H2: The level of privacy concerns is negatively related to self-disclosure.

H3: The level of privacy concerns is negatively related to friending.

Self-efficacy in managing privacy settings and privacy protection

Although some studies have found a positive relationship between privacy concerns and privacy protection, many other studies have also documented a ''privacy paradox'' on SNSs.[2,3,26] Trust, a confidence belief that users' personal information submitted to the service provider can be handled

reliably and safely, plays a positive role in influencing willingness to disclose personal information in the privacy calculus model.[14,24,35] As SNSs require personal information disclosure, trust becomes an important consideration; it reduces perceived risks involved in revealing private information.[14] If the level of trust exceeds the level of perceived risk, SNS users are likely to engage in risky behavior. Trust, as a confidence belief, can be identified in the relationship between users and service providers, and it can also be found in SNS users regarding the extent to which they consider themselves able to handle personal information reliably and safely on SNS.[24] It is worth noting that individuals' confidence in their own ability to manage privacy settings is closely related to, and sometimes used interchangeable with, the concept of self-efficacy in privacy management—the perception of one's ability to protect one's privacy.[36–38]

Literature on privacy self-efficacy has produced mixed findings in the online environment. For example, studies of online consumer behavior have shown that privacy self-efficacy enhances privacy protecting behaviors and lessens self-disclosure,[36,39] which is different from what the privacy calculus model proposes regarding the relationship between trust/confidence beliefs and disclosing information. Other studies, more in line with the privacy calculus model, suggest that privacy self-efficacy can help to explain the ''experience effect''—that as users gain more online experience, they become less concerned about privacy and more willing to share personal information.[37,40] Users with high levels of privacy self-efficacy would have lower estimates of risk.[36] As users' confidence grows in their ability to protect themselves from privacy invasion, they believe that they can thwart or counteract the negative consequences of privacy invasion that result from their usage behaviors.[36,37]

As the potential threats to privacy on SNSs have prompted concerns, some SNSs have given users more control over who can see or use their information by making parts of their profile off limits to the public. However, some SNSs have made privacy settings hard to find, difficult to understand, easy to dismiss, and cumbersome to adjust.[41] For instance, Facebook has frequently changed what personal information is visible and how it is classified.[5] This discourages users from protecting privacy.[5]

This study, therefore, explores the role of users' self-efficacy in perceiving themselves as being able to manage the settings for privacy protection. Given that two different arguments and findings were documented in previous studies, this study asks:

RQ1: How does users' self-efficacy in privacy management on SNSs relate to (a) limiting profile visibility, (b) self-disclosure, and (c) friending?

Given that users will weigh costs against benefits in determining whether to disclose information on SNSs, self-efficacy in privacy management may moderate the influence of privacy concerns on adopting different strategies to protect privacy. Examining the interaction relationship can help to provide an explanation for the privacy paradox that users' concerns over privacy risks do not always promote them to protect privacy.[1,3,4,26,42] It is possible that users' self-efficacy in their ability to deal with the consequences of privacy invasion may buffer their privacy concerns and thus weaken the positive effect of privacy concerns on privacy protection. This study therefore asks:

RQ2: How does users' self-efficacy in privacy management moderate the effect of privacy concerns on (a) limiting profile visibility, (b) self-disclosure, and (c) friending?

Method

Sample and procedure

Given that many SNS users are young people who are likely to engage in SNSs, this study focuses on college students.[43–46] This provides a unique opportunity to understand privacy on SNSs. The research subjects were college students in two introductory courses at a large public university in the Southwest United States. The courses were chosen because they primarily attract first-year students across the campus, and the course instructors (who were not connected to the project) kindly allowed access to the field and offered credit points as an incentive to encourage students to participate in the survey. A Web link for the survey was announced in class and also sent out to the students via e-mail. Between November 6 and December 10, 2011, 559 students (out of 630 enrolled) filled out the survey, yielding a response rate of 89%. Listwise deletion was adopted in the analysis. Thus, the results include only respondents giving valid answers on all variables involved, giving a total of 515 students.

Measurement

Privacy concern was measured with one item adopted from prior studies.[32] Respondents were asked to indicate the extent to which they were ''concerned about their privacy on SNSs'' using a 5-point Likert scale ranging from 1 = ''strongly disagree'' to 5 = ''strongly agree'' ($M = 3.61$, $SD = 1.11$). Self-efficacy in privacy management was measured by asking respondents to what extent they are confident in (a) blocking spam or unwanted content, (b) adjusting privacy settings, and (c) managing personal profiles on SNSs. Respondents answered on a 5-point Likert scale ranging from 1 = ''strongly disagree'' to 5 = ''strongly agree'' ($\alpha = 0.78$, $M = 4.42$, $SD = 0.66$). Limiting profile visibility was measured by asking respondents the extent to which they (a) restrict access to their full profile, (b) limit who can see certain information such as photos or posts, and (c) read the details of the privacy statements for limiting profile visibility, using a 5-point Likert scale ranging from 1 = ''strongly disagree'' to 5 = ''strongly agree'' ($\alpha = 0.86$, $M = 3.68$, $SD = 0.84$). Respondents were asked to indicate the frequency of (a) accepting friend invitations, (b) offering friend invitations, and (c) building relationships with people on SNSs using a 5-point Likert scale ranging from 1 = ''never'' to 5 = ''daily'' to capture friending behaviors ($\alpha = 0.70$, $M = 3.32$, $SD = 0.67$). Regarding self-disclosure, respondents were asked about the frequency, in the previous 30 days, of doing the following on SNSs: (a) updating status; (b) uploading and sharing photos; (c) sharing Web links, news stories, blog posts, and notes; and (d) sharing location. They answered using a 7-point Likert scale ranging from 1 = ''never'' to 7 = ''a few times an hour'' ($\alpha = 0.81$, $M = 3.00$, $SD = 1.03$). Control variables included gender (50% of each),

ethnicity (51.9% white, 5% black, 13.6% Hispanic, 16.8% Asian, and 12.7% other), and Facebook network size (after square root transformation: $M = 25.57$, $Mdn = 25.50$, $SD = 9.09$, skewness = 0.84) for potential confounding effects, as they have been documented to be associated with SNS use, privacy concerns, and privacy protection.[8,42,47–49]

Results

To examine simultaneous regression of multiple dependent variables, and assess the overall model fit, the model in Figure 1 was tested using path analysis in Mplus 7. Before conducting path analysis, several underlying assumptions (normality, sampling adequacy, and no extreme multicollinearity) were checked. The chi-square statistic of the model was insignificant ($\chi^2 = 10.29$, $df = 6$, $p = 0.11$), which indicated an adequate fit between the overall model and the observed data. The model also fit the data well across model goodness-of-fit indexes. The Bentler comparative fit index was 0.995, the Tucker–Lewis index was 0.990, the root mean square error of approximation was 0.02, and the standardized root mean square residual was 0.03.

As shown in Figure 1, H1, which proposed that the level of privacy concerns was positively related to limiting profile visibility, was supported ($\beta = 0.48$, $p < 0.001$). However, H2, which assumed a negative relationship between privacy concerns and self-disclosure, was not supported. Concerning the negative relationship between privacy concerns and friending, the findings supported H3 ($\beta = -0.08$, $p < 0.05$). Regarding the effect of self-efficacy in privacy management on limiting profile visibility (RQ1a), self-efficacy in privacy management was significantly and positively related to limiting profile visibility ($\beta = 0.08$, $p < .05$). Interestingly, when it comes to self-disclosure (RQ1b), self-efficacy in privacy management was positively related to self-disclosure ($\beta = 0.08$, $p < 0.05$). In terms of the effect of self-efficacy in privacy management on friending (RQ1c), self-efficacy in privacy management was not significantly associated with friending.

To answer RQ2 regarding the interaction effects between privacy concerns and self-efficacy in privacy management on limiting profile visibility (RQ2a), self-disclosure (RQ2b), and friending (RQ2c), hierarchical regressions were conducted with control variables entered in the first block, the main effects of privacy concerns and self-efficacy in privacy management in the second block, and the interaction term in the third block. As shown in Table 1, the interaction effect was only significant in friending. Self-efficacy in privacy management significantly moderated the relationship between privacy concerns and friending ($\beta = -1.14$, $p < 0.01$). Figure 2 presented this interaction relationship, suggesting that for those highly concerned about privacy, self-efficacy in privacy management played a significant role in constraining friending on SNSs. However, for those with a low level of privacy concerns, friending behaviors were boosted by their self-efficacy in managing privacy setting.

Discussion and Conclusions

Although SNSs provide a myriad of gratifications, such as personal fulfillment, social interaction, and self-presentation,[43,46,50] they have generated concerns about privacy risks.[24,51] Building on mixed finding regarding the relationships between privacy concerns, SNS usage, and privacy-protecting behaviors, the present study examines whether and how privacy concerns and efficacy in one's own ability to manage privacy settings affect different privacy-protecting behaviors on SNSs, including limiting profile visibility, self-disclosure, and friending.

Based on how users weigh costs and benefits in determining privacy protection in the privacy calculus model, this study finds privacy concerns associated with users protecting their privacy by limiting their profile visibility and constraining their friending behaviors. Individuals who are concerned about their privacy can engage in protective behaviors, such as setting the visibility of a personal profile and limiting who can see certain information. Privacy concerns are also associated with less friending—a network-expanding behavior that has been considered a privacy risk-taking behavior.[10]

While previous studies have produced inconsistent findings in the relationship between self-efficacy in privacy management and privacy-protecting behaviors,[34,35] this study finds that self-efficacy in privacy management can work as either

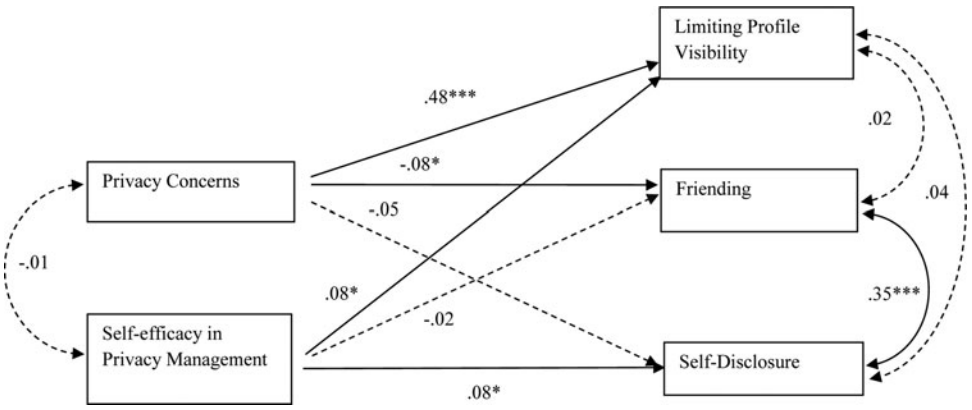

FIG. 1. Model testing how privacy concerns and self-efficacy in privacy management influence limiting profile visibility, self-disclosure, and friending. Note: $n = 515$. Path entries are standardized coefficients (betas). Goodness of fit: $\chi^2 = 10.29$, $df = 6$, $p = 0.11$; root mean square error of approximation = 0.02; comparative fit index = 0.995; Tucker–Lewis index = 0.990; standardized root mean square residual = 0.03. Gender, ethnicity, and network size are included in the model as control variables. Dotted paths reveal a nonsignificant relationship. *$p < 0.05$; ***$p < 0.001$.

Table 1. Interaction Effect Between Privacy Concerns and Self-Efficacy in Privacy Management on Limiting Profile Visibility, Self-Disclosure, and Friending

	Limiting profile visibility	*Self-disclosure*	*Friending*
Block 1: Control variables			
Gender	0.27***	0.12**	−0.03
White	−0.06	−0.16***	−0.01
Network size	−0.05	0.21***	0.43***
Incremental R^2 (%)	8.0***	6.9***	18.5***
Block 2: Main effect			
Privacy concerns	0.48***	−0.04	−0.08*
Self-efficacy in privacy management	0.08*	0.08*	0.02
Incremental R^2 (%)	22.1***	1.0	0.8
Block 3: Interaction effect			
Privacy concerns × self-efficacy in privacy management	0.32	−0.46	−1.14**
Incremental R^2 (%)	0.1	0.3	1.7*
Total R^2	30.2***	8.2***	21.0***

Entries are OLS standardized coefficients. *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

a cost or benefit depending on the privacy-protecting strategies users choose to adopt. Self-efficacy in privacy management is positively associated with limiting profile visibility. However, self-efficacy in privacy management aligns with self-disclosure. It indicates that when users are confident in themselves as adept at adjusting privacy settings and controlling their personal information, they manage audiences via privacy settings and limit with whom they share information. However, they do not lessen their self-disclosure. Instead, they still disclose more personal information on SNSs to these smaller audiences. It is possible that when users are confident about handing problems related to privacy invasion, and when they limit their profile visibility, they do not consider the personal information they share to be at privacy risk.

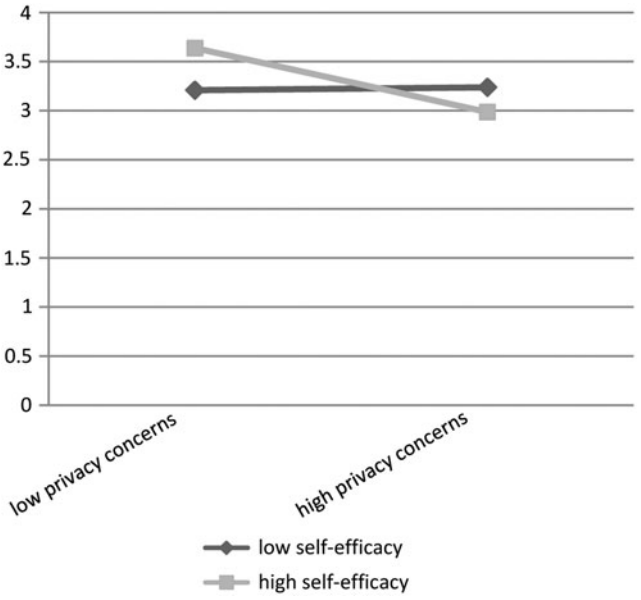

FIG. 2. The interaction effect of privacy concerns and self-efficacy in privacy management on friending.

Although there is no main effect from self-efficacy in privacy management on friending behaviors, the results uncover evidence that self-efficacy in privacy management plays a significant moderating role in influencing the relationship. The pattern suggests that self-efficacy in privacy management influences users' friending behavior in a different way, depending on users' level of privacy concerns.

While previous studies indicated a privacy paradox—the fact that privacy concerns do not constrain SNS use—the interplay between privacy concerns and self-efficacy in privacy management suggests that the self-efficacy in privacy management can outweigh the privacy concerns for those with low privacy concern and encourage users' friending behaviors. Activities related to network expanding can be limited only when users are high in both self-efficacy in privacy management and privacy concerns. Our findings on the role of self-efficacy in privacy management and the interaction effect fill the gap in the body of research on social network privacy, given that self-efficacy in privacy management on SNSs has received little attention.

This research has limitations that call for future research. First, the data are cross-sectional. Although an alternative model is additionally tested with the directions of causal paths reversed to ensure the proposed model fit the data best, a causal relationship could not be confirmed between the variables. Panel data are needed to provide a better understanding of the causal direction. In addition, the sample is limited to college students, which hinders the generalizability of the results. Given that a large number of users are college students, the results, however, provide a meaningful examination of those with high levels of participation in SNSs. Future research examining other groups may not provide findings from proficient SNS users as this study does.

Furthermore, users can adopt other strategies to protect their privacy, such as self-censorship, ranging from posting socially appropriate content to deleting controversial posts or untagging photos that may turn off future employers.[50] Users can also use false information to avoid privacy risk.[26] Therefore, other types of privacy-protecting behaviors can be included in the model in future research. In addition to privacy concerns and self-efficacy in privacy management, other factors that may influence individuals' privacy-protecting behaviors, such as network tie strength, social capital, and gratifications sought, could be included in the relationship for future study.[10,43]

Despite these limitations, this research has extended the existing studies on SNS privacy, and has also provided scholarly and practical implications. First, the findings suggest that strategies of privacy protection, including limit profile visibility, self-disclosure, and friending, can be affected by privacy-related variables through different processes. It is possible that users take action to protect their information from privacy risks but at the same time actively and intensely engage in social networking on SNSs. In addition, self-efficacy in privacy management should be boosted with caution for two reasons. First, high self-efficacy in privacy management and low privacy concerns can enhance individuals' network expanding, a privacy risk-taking behavior on SNSs. Second, as college students and teens are

often considered more tech savvy than those in other age groups, they are likely to have higher self-efficacy in privacy management in social media use. But to what extent they are concerned about their privacy on SNSs, and whether their privacy concern is high enough to prompt privacy-protecting behaviors and reduce risk-taking behaviors on SNSs, is questionable. To conclude, a way to enhance not only self-efficacy in privacy management but also privacy concerns is needed.

Acknowledgments

The research draws data from the Social Media in Student Life Project funded by the Office of the Vice President for Research, The University of Texas at Austin, and the Undergraduate Research Mentorship Award, College of Communication, The University of Texas at Austin.

Author Disclosure Statement

No competing financial interests exist.

References

1. boyd dm, Ellison NB. Social network sites: definition, history, and scholarship. Journal of Computer-Mediated Communication 2007; 13:210–230.
2. Acquisiti A, Gross R. (2006) Imagined communities: awareness, information sharing, and privacy on the Facebook. In Golle P, Danezis G, eds. *Proceedings of 6th Workshop on Privacy Enhancing Technologies*. Cambridge, England: Robinson College, pp. 36–58.
3. Debatin B, Lovejoy JP, Horn A-K, et al. Facebook and online privacy: attitudes, behaviors, and unintended consequence. Journal of Computer-Mediated Communication 2009; 15:83–108.
4. Livingstone S. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy, and self-expression. New Media & Society 2008; 10:393–411.
5. Madden M. (2012) Privacy management on social network sites. Pew Internet & American Life Project. www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/ (accessed Dec. 10, 2013).
6. Rainie L, Lenhart A, Smith A. (2012) The tone of life on social networking sites. Pew Internet & American Life Project. www.pewinternet.org/2012/02/09/the-tone-of-life-on-social-networking-sites/ (accessed Dec. 15, 2013).
7. Taddicken M. The ''Privacy Paradox'' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication 2013; 19:248–273.
8. 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 2009; 12:341–345.
9. Bultman M. (2012) Facebook IPO to make Dobbs Ferry's Mark Zuckerberg a $24 billion man. http://greenburgh.dailyvoice.com/news/facebook-ipo-make-dobbs-ferrys-mark-zuckerberg (accessed Feb. 3, 2014).
10. Ellison NB, Vitak J, Steinfield C, et al. (2011) Negotiating privacy concerns and social capital needs in a social media environment. In Trepte S, Reinecke L, eds. *Privacy online: perspectives on privacy and self-disclosure in the social web*. New York: Springer, pp. 19–32.
11. Warren S, Brandeis L. The right to privacy. Harvard Law Review 1890; 4:193–220.
12. Fried C. Privacy. Yale Law Journal 1968; 77:475–493.
13. Westin A. (1967) *Privacy and freedom*. New York: Atheneum.
14. Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. Information Systems Research 2006; 17:61–80.
15. Dinev T, Bellotto M, Hart P, et al. Privacy calculus model in e-commerce: a study of Italy and the United States. European Journal of Information Systems 2006; 15:389–402.
16. Zhao S, Grasmuck S, Martin J. Identity construction on Facebook: digital empowerment in anchored relationships. Computers in Human Behavior 2008; 24:1816–1836.
17. Goel V. Some privacy, please? Facebook, under pressure, gets the message. The New York Times, 2014. www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html?_r=0 (accessed Aug. 25, 2014).
18. Jiang ZJ, Heng CS, Choi BCF. Privacy concerns and privacy-protective behaviors in synchronous online social interactions. Information Systems Research 2013; 24:579–595.
19. Ajzen I. The theory of planned behavior. Organizational Behavior & Human Decision Processes 1991; 50:179–211.
20. Baek YM, Kim E-m, Bae Y. My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns. Computers in Human Behavior 2014; 31:48–56.
21. Yang S, Wang Y, Wang K-l. The influence of information sensitivity compensation on privacy concern and behavioral intention. The Database for Advances in Information Systems 2009; 2009:1.
22. Baek YM. Solving the privacy paradox: a counter-argument experimental approach. Computers in Human Behavior 2014; 38:33–42.
23. Jang SM. Challenges to selective exposure: selective seeking and avoidance in a multitasking media environment. Mass Communication & Society 2014; 17:665–688.
24. Krasnova H, Veltri NF, Günther O. Self-disclosure and privacy calculus on social networking sites: the role of culture. Business & Information Systems Engineering 2012; 4:127–135.
25. Culnan MJ, Bies RJ. Consumer privacy: balancing economic and justice considerations. Journal of Social Issues. 2003; 59:323–342.
26. Tufekci Z. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society 2008; 28:20–36.
27. Krasnova H, Veltri NF. (2010) Privacy calculus on social networking sites: explorative evidence from Germany and USA. Proceedings of the 43rd Hawaii International Conference on System Sciences, Koloa, HI.
28. Youn S, Hall K. Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. CyberPsychology & Behavior 2008; 11:763–765.
29. Moscardelli DM, Divine R. Adolescents' concern for privacy when using the Internet: an empirical analysis of predictors and relationships with privacy-protecting behaviors. Family & Consumer Sciences Research Journal 2007; 35:232–252.
30. Sheehan KB, Hoy MG. Flaming, complaining, abstaining: how online users respond to privacy concerns. Journal of Advertising 1999; 28:37–51.

31. Milne GR, Culnan MJ. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing 2004; 18:15–29.
32. Youn S. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs 2009; 43:389–418.
33. Feng Y, Xie W. Teen's concern for privacy when using social networking sites: an analysis of socialization agents and relationships with privacy-protecting behaviors. Computers in Human Behavior 2014; 33:153–162.
34. Aldhafferi N, Watson C, Sajeev ASM. Personal information privacy setting of online social networks and their suitability for mobile Internet devices. International Journal of Security, Privacy & Trust Management 2013; 2:1–17.
35. Dwyer C, Hiltz SR. (2007) Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems. Keystone, CO.
36. LaRose R, Rifon NJ. Promoting i-Safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. Journal of Consumer Affairs 2007; 41: 127–149.
37. Rifon NJ, LaRose R, Choi SM. Your privacy is sealed: effects of web privacy seals on trust and personal disclosure. Journal of Consumer Affairs 2005; 39:339–362.
38. Bandura A. (1997) *Self-efficacy: the exercise of control*. New York: Freeman.
39. Lwin MO, Williams JD. A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. Marketing Letters 2004; 14:257–272.
40. Miyazaki AD, Fernandez A. Consumer perceptions of privacy and security risks for online shopping. Journal of Consumer Affairs 2001; 35:27–44.
41. boyd dm, Hargittai E. Facebook privacy settings: who cares? First Monday 2010; 15.
42. Lewis K, Kaufman J, Christakis N. The taste for privacy: an analysis of college student privacy setting in an online social network. Journal of Computer-Mediated Communication 2008; 14:79–100.
43. Chen H-T, Kim Y. Problematic use of social network sites: the interactive relationship between gratifications sought and privacy concerns. Cyberpsychology, Behavior, & Social Networking 2013; 16:806–812.
44. Steinfield C, Ellison NB, Lampe C. Social capital, self-esteem, and use of online social network sites: a longitudinal analysis. Journal of Applied Developmental Psychology 2008; 29:434–445.
45. Ellison. NB, Steinfield C, Lampe C. The benefits of Facebook ''friends'': social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication 2007; 12.
46. Kim Y, Sohn D, Choi SM. Cultural difference in motivations for using social network sites: a comparative study of American and Korean college students. Computers in Human Behavior 2011; 27:365–372.
47. Lenhart A, Madden M. (2007) Social networking websites and teens: an overview. Pew Internet & American Life Project. www.pewinternet.org/files/old-media//Files/Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf.pdf (accessed Nov. 20, 2013).
48. Fogel J, Nehmad E. Internet social network communities: risk taking, trust, and privacy concerns. Computers in Human Behavior 2009; 25:153–160.
49. Joinson AN, Paine C, Buchanan T, et al. Measuring self-disclosure online: blurring and non-response to sensitive items in web-based surveys. Computers in Human Behavior 2008; 24:2158–2171.
50. Borneo N, Barkhuus L. (2011) Privacy management in a connected world: students' perception of Facebook privacy setting. ACM conference on Computer Supported Cooperative Work (CSCW '11), Hangzhou, China.

Address correspondence to:
Dr. Hsuan-Ting Chen
School of Journalism and Communication
The Chinese University of Hong Kong
Shatin
Hong Kong

E-mail: htchen@cuhk.edu.hk