The Influence of Privacy Protection Self-Efficacy on Privacy Behavior of Social Network Users: A Postprint Study

Authors: Xu Yiming, Li He, Yu Lu

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] The frequent occurrence of data leakage incidents has led an increasing number of social network users to question the effectiveness of their privacy protection behaviors, and even to abandon privacy protection strategies. This study investigates the reasons behind social network users' abandonment of privacy protection behaviors from the perspective of privacy protection self-efficacy. [Method/Process] This study reviews self-efficacy literature, introduces privacy fatigue as a mediating variable, constructs a structural equation model, and collects and analyzes data through questionnaire surveys. [Results/Conclusion] The privacy protection self-efficacy of social network users does not directly influence their privacy protection disengagement behaviors; rather, it exerts indirect effects through the complete mediating variable of privacy fatigue. Privacy protection self-efficacy from different sources yields differential effects.

Full Text

Preamble

Vol. 63 No. 17, September 2019
ChinaXiv Cooperative Journal

Research on the Influence of Privacy Protection Self-Efficacy on Privacy Behaviors of Social Network Users

Xu Yiming, Li He, Yu Lu
School of Management, Jilin University, Changchun 130022

Abstract

[**Purpose/Significance**] Frequent data leakage incidents have led increasing numbers of social network users to question the effectiveness of their privacy protection behaviors, even prompting them to abandon privacy protection strategies. This study explores the reasons why social network users abandon privacy protection behaviors from the perspective of privacy protection self-efficacy. [**Method/Process**] By reviewing relevant literature on self-efficacy, privacy fatigue was introduced as a mediating variable to establish a structural equation model, with data collected and analyzed through questionnaire surveys. [**Result/Conclusion**] Privacy protection self-efficacy among social network users does not directly influence privacy protection disengagement behavior; rather, it exerts indirect effects through the complete mediating variable of privacy fatigue. Different sources of privacy protection self-efficacy produce different impacts.

Keywords: privacy protection; self-efficacy; privacy fatigue; disengagement behavior; privacy behavior
Classification Number: C913.4
DOI: 10.13266/j.issn.0252-3116.2019.17.015

Introduction

Privacy is defined differently across countries and cultures [1]. Generally, privacy is considered part of human rights, with established classification standards for assessing potential harm from violations [2]. With the development and widespread use of information technology, privacy issues have become a major focus of interdisciplinary research between internet technology and social sciences [3]. In 2016, global data breach reports reached 4,149 incidents, involving 420 million records [4]. A 2017 survey by GIGYA [5] showed that 69% of consumers in the UK and US were concerned about device security and privacy risks, while 68% expressed distrust in how online service providers handle personal information. Similar issues exist in China, where the "2018 Kantar China Social Media Impact Report" [6] indicated that 44% of social media users expressed concerns about their information security. These data demonstrate that people cannot control whether their online information will be leaked. Amid frequent data breaches, many believe they lack effective means to protect personal information disclosed online [7] and consequently abandon privacy protection strategies [8]. Increasingly complex personal network privacy protection measures are exacerbating this sense of control loss and abandonment behavior [9].

When studying user privacy interference, many scholars treat information disclosure behavior as a final outcome. However, beyond disclosing personal information, social network users may also adopt protective measures against privacy violations, such as complaints and negative reviews [10].

Behavioral disengagement refers to the phenomenon where individuals reduce effort or even abandon original goals when facing stress [11], ultimately leading to

withdrawal from activities [12]. In the context of social network privacy, H. Choi et al. [13] defined users' reduction in response efforts when facing privacy threats as "privacy protection disengagement"—the abandonment of privacy protection measures, including actively deleting information, deliberately providing false personal information, spreading negative word-of-mouth, and complaining to companies or third-party organizations. Research shows [14] that most Facebook users do not read website privacy policies, and most college students do not restrict others' access to their personal profiles, instead using default settings (i.e., open access to everyone on the website) [15]. S. Preibusch et al. [16] found that excessive disclosure of personal information is very common among internet users, yet users cannot fully supervise how social network providers use their information [17].

Self-efficacy (SE) refers to an individual's confidence or belief in their ability to complete a specific task [18]. N. J. Rifon et al. [19] found that computer self-efficacy is significantly associated with two important components of user privacy concern: collection of personal data and unauthorized secondary use. H. S. Rhee et al. [20] discovered that information protection self-efficacy positively correlates with information security awareness. However, domestic and international research on privacy protection self-efficacy in social networks remains scarce, with general studies suggesting that privacy protection self-efficacy plays a moderating role in different contexts. H. H. Lee et al. [21] examined the moderating effect of privacy self-efficacy on the relationship between mobile users' perceived relevance/perceived risks of location-based mobile marketing and their avoidance intentions/methods. R. LaRose et al. [22] also demonstrated that while privacy protection self-efficacy does not directly affect online shoppers' privacy disclosure, it moderates the impact of privacy warnings and consumers' perceptions of privacy concerns or privacy barriers.

In summary, this study aims to: (1) clarify the concept and dimensions of privacy protection self-efficiency, and (2) empirically test its role in social network users' privacy protection disengagement behavior.

Theoretical Foundation

Privacy protection is a persistent challenge for internet users. Over time, maintaining personal privacy has become a burden. In the digital age, personal data collection and sharing have become very easy, making it difficult to control how personal information is used and to maintain privacy.

2.1 Privacy Protection Self-Efficacy

Self-efficacy is an important factor in individual motivation, affecting thinking, motivation [23], expected performance [24], and perseverance in the face of challenges [25-26]. Privacy protection self-efficacy refers to an individual's perceived ability to control personal boundaries in order to protect personal information and space [27].

Attribution theory suggests that individuals' beliefs about their performance vary with the controllability of outcomes [28], attributing success (or failure) to themselves (internal) or other environmental factors (external) [29]. The differential impacts of internally versus externally sourced self-efficacy on individual behavior have been demonstrated in other fields [30]. Therefore, this study distinguishes between internal and external dimensions of privacy protection self-efficacy.

Internal privacy protection self-efficacy represents individuals' belief in their own ability to independently protect their privacy. Like a user familiar with appliances who believes they don't need to read manuals, some social network users believe they can protect their privacy information based on prior experience. When internal privacy protection self-efficacy is high, individuals are less dependent on external support to learn or guide their privacy protection behaviors. Therefore, we define internal privacy protection self-efficacy as individuals' belief in their ability to protect their privacy.

External privacy protection self-efficacy represents individuals' belief in protecting their privacy information, not based on their own experience or ability, but from external sources such as assistance from others. Research shows [31] that people's beliefs about their abilities are influenced by other social roles they can reference, which sometimes can be computers [32] rather than humans. When engaging in privacy protection behaviors, individuals can learn by imitating others' behaviors or accepting guidance from other social roles. Therefore, this study defines external privacy protection self-efficacy as individuals' belief that they can complete privacy protection with support from at least one social role.

2.2 Privacy Behavior

2.2.1 Privacy Protection Disengagement When facing privacy threats, social network users may adopt protective approaches to enhance their management of personal information, including restricting information scope, posting false information, and carefully studying website privacy agreements. However, increasing difficulty of privacy protection and frequent data breaches may make people feel they cannot control their personal information, ultimately leading them to abandon privacy protection behaviors [8] and resulting in privacy protection disengagement. This phenomenon indicates that users abandon various response behaviors when facing privacy threats.

2.2.2 Privacy Fatigue When individuals are required to process more information in decision-making than they can handle, they often experience "fatigue" [33]. Fatigue stems from facing high demands and unattainable goals, with the primary deficit being inability to make decisions. Previous fatigue research also shows that fatigue leads to inability to cope and avoidance behavior [34]. Privacy fatigue reflects internet users' burnout regarding privacy issues, caused by the complexity of online privacy protection and underestimation of data breach risks, which reduces user attention to privacy issues [35]. People who feel fa-

tigued about privacy leaks reduce their decision-making effort for privacy protection [36]. On the internet, privacy-related statements and agreements have become increasingly complex and obscure, requiring users to invest substantial effort in managing their online personal information. This likely leads users to abandon attempts to understand privacy agreements [37], directly checking "I accept," especially when they need to click links to view the full text [37].

Research Model and Hypotheses

3.1 Privacy Fatigue and Privacy Protection Disengagement

The purpose of social network users' privacy protection behaviors is to prevent their privacy information from being misused. Therefore, when facing privacy threats, non-action may seem illogical. Particularly, individuals with higher privacy concerns are more likely to resist companies that threaten their privacy, such as through complaints or deleting personal information from service providers [10]. However, fatigued individuals typically seek to minimize decision-making effort, tending to reduce behavioral motivation in tasks rather than seeking solutions [38], even willing to forgo potential benefits [39]. Some studies emphasize that disengagement is a key outcome of fatigue [40-41]. Therefore, social network users experiencing privacy fatigue may abandon proactive behaviors to address privacy threats. Thus, this study hypothesizes:

H1: Among social network users, privacy fatigue is positively correlated with privacy protection disengagement.

3.2 Privacy Protection Self-Efficacy and Privacy Fatigue

Social network users provide personal information to service providers to use social network services. In this relationship, users cannot fully supervise how service providers use information. To build user trust, most companies provide privacy policy statements and privacy protection services. However, the complexity of privacy protection systems may require social network users to invest excessive effort, as failure to do so prevents them from making decisions about online privacy information, potentially causing user fatigue and leading to privacy issues [45].

Extensive research shows that self-efficacy plays an important role in influencing users' perception and use of technology [42], can reduce users' anxiety about technology [43], and is an important reference for users' assessment of perceived avoidance ability [44]. Evidence shows that self-efficacy affects individuals' learning ability, expected performance, and perseverance when facing challenges [25]. Individuals with higher self-efficacy are more committed to achieving goals [45] and can persist when facing difficulties [46]. A. Bandura et al. found that individuals with high self-efficacy treat obstacles as learning experiences [47] to sharpen their perseverance. Medical researchers have found that self-efficacy can reduce negative emotions like fatigue in cancer patients [48].

External privacy protection self-efficacy reflects belief in the ability to use external assistance. When individuals believe they can complete tasks with assistance, they may not generate optimistic assessments of current difficulties. On the other hand, people typically attribute success to internal rather than external factors [49], while internal sources of self-efficacy are primarily personal success experiences [50]. Compared to individuals with high internal privacy protection self-efficacy, those with high external privacy protection self-efficacy may have fewer success experiences to draw from. Therefore, external privacy protection self-efficacy may not improve individuals' understanding and confidence in adopting strategies and activities when facing privacy threats. In summary, this study hypothesizes:

H2: Among social network users, internal privacy protection self-efficacy is negatively correlated with privacy fatigue.

H3: Among social network users, external privacy protection self-efficacy is not correlated with privacy fatigue.

3.3 Privacy Protection Self-Efficacy and Privacy Protection Disengagement

Frequent data breaches are not only increasing privacy concerns but also affecting public underestimation or neglect of risks. H. Cho et al. [51] found that individuals show strong optimistic bias about online privacy risks, believing they are less vulnerable than others. This finding was also confirmed in Y. M. Baek et al.'s study [52]. However, this optimistic estimate is not due to social network users' own success experiences or abilities but rather from observations and judgments of the network environment and others, thus belonging to external privacy protection self-efficacy.

On the other hand, high self-efficacy can positively affect behavioral intentions, while low self-efficacy positively affects avoidance intentions because individuals believe they lack the ability to fully overcome specific threats [54]. However, due to the existence of the privacy paradox [55], internet users' privacy protection intentions hardly affect their privacy protection behaviors [56]. Therefore, the link between social network users' internal privacy protection self-efficacy and their privacy protection behavior remains uncertain. In summary, this study hypothesizes:

H4: Among social network users, internal privacy protection self-efficacy is not directly correlated with privacy protection disengagement.

H5: Among social network users, external privacy protection self-efficacy is positively correlated with privacy protection disengagement.

3.4 Research Model

Based on the hypotheses proposed above, the research model is established as shown in [Figure 1: see original paper].

[Figure 1: see original paper] Research Model and Hypothesized Relationships

Research Methods

This study primarily collected data through questionnaires, used SPSS 21.0 for data organization and statistical analysis, constructed a PLS-SEM model, and employed WarpPLS for path analysis and hypothesis testing to obtain research results.

4.1 Questionnaire Design

This study collected data on online users' privacy protection through questionnaires to validate the proposed conceptual model. Measurement items used a 7-point Likert scale (1 = "strongly disagree," 7 = "strongly agree"), with specific measurement items adapted from mature scales used in other scholars' research. Detailed survey content and measurement item sources are shown in .

Questionnaire Measurement Items and Sources

Construct	Measurement Item	Source
Privacy Protection Self-Efficacy (Internal) (I-PSE)	I can protect my privacy without guidance	[30]
	I can protect my privacy without prior experience with similar websites	
	I can protect my privacy with only website usage help	
Privacy Protection Self-Efficacy (External) (E-PSE)	I can protect my privacy if someone can help when I encounter problems	[30]
	I can protect my privacy if someone can guide me on how to start	
	I can protect my privacy if someone can give me a demonstration	
	I can protect my privacy if the website I use is reliable	
Privacy Fatigue (PF)	I feel down when dealing with privacy issues in social network environments	[13]
	I am tired of social network privacy protection issues	
	Caring about social network privacy is annoying to me	

Construct	Measurement Item	Source
Privacy Protection Disengagement (PD)	I am becoming less interested in social network privacy issues I have become less enthusiastic about protecting my personal information provided to online service providers I have begun to doubt the importance of social network privacy issues If my personal information provided to online service providers is misused, I will not consider addressing this issue If my personal information provided to online service providers is misused, I will give up on the idea of solving this problem If my personal information provided to online service providers is misused, I will give up trying to solve this problem	[13]

4.2 Descriptive Statistics

Questionnaires were distributed online, with 347 responses collected. Strict criteria were applied to screen and clean the collected questionnaires: (1) sample users who had not used social networks; (2) sample users who did not have their own social network accounts; (3) contradictory responses to similar items; (4) data with large-scale (>80%) identical responses; (5) completion time below 120 seconds. After cleaning, 301 valid questionnaires were obtained, with an effective response rate of 86.7%. Sample characteristics are shown in .

Sample Descriptive Statistics

Category	Subcategory	Count	Percentage (%)
Age	Under 18	64	21.26
	18-25	91	30.23
	26-30	79	26.25
	31-40	92	30.56
	41-50	43	14.29
	51-60	33	10.96

Category	Subcategory	Count	Percentage (%)
Highest Education (including current)	High school and below	36	11.98
	Undergraduate	136	45.18
	Master's	91	30.23
	Doctoral	38	12.62
Occupation	Full-time student	36	11.98
	Technical/R&D personnel	24	7.97
	Market/PR personnel	22	7.31
	Administrative/Logistics personnel	21	6.98
	Financial/Audit personnel	20	6.64
	Clerical/Office personnel	19	6.31
	Consultant/Advisor	18	5.98
	Professional (e.g., accountant, lawyer, architect, medical staff, journalist, etc.)	13	4.32

The age and education distributions of respondents basically satisfy normal distribution, indicating relatively uniform stratification. Undergraduate users were the largest group (45.18% of total), and 77.74% of respondents were aged 18-40, consistent with the characteristic that highly educated and young users are the main internet user groups. Occupationally, distribution was relatively even, with all occupations below 8% except students (11.98%), indicating relatively uniform occupational coverage.

4.3 Measurement Model Validation

First, the reliability and validity of the questionnaire were assessed, as shown in .

Factor Loadings, Alpha, CR, and AVE of Measurement Items

Construct	Item	Factor Loading	Cronbach's α	Cronbach's α if Item Deleted	CR	AVE
Privacy Protection Self-Efficacy (Internal) (I-PSE)	I-PSE1	0.774	0.881	0.853	0.919	0.790
	I-PSE2	0.919		0.904		
	I-PSE3	0.895		0.857		
Privacy Protection Self-Efficacy (External) (E-PSE)	E-PSE1	0.858	0.900	0.890	0.928	0.718
	E-PSE2	0.878		0.864		
	E-PSE3	0.844		0.900		
	E-PSE4	0.785		0.915		
Privacy Fatigue (PF)	PF1	0.940	0.956	0.957	0.966	0.628
	PF2	0.951		0.940		
	PF3	0.937		0.945		
	PF4	0.905		0.950		
	PF5	0.966		0.947		
	PF6	0.947		0.950		
Privacy Protection Disengagement (PD)	PD1	0.797	0.951	0.873	0.700	0.875
	PD2	0.785		0.800		

Construct	Item	Factor Loading	Cronbach's α	Cronbach's α if Item Deleted	CR	AVE
	PD3	0.800		0.785		

Composite reliability (CR) was used to test questionnaire reliability, while average variance extracted (AVE) and Cronbach's α coefficient were used to test scale validity. First, all constructs had CR values greater than 0.8, indicating good indicator reliability. Cronbach's α coefficients were all greater than 0.7, indicating good internal consistency. AVE values were all greater than 0.7, indicating good convergent validity. Then, discriminant validity was tested by comparing the square root of each factor's AVE with inter-variable correlation coefficients, as shown in .

Validity Analysis of Discriminant Factors

Variable	I-PSE	E-PSE	PF	PD
I-PSE	0.889			
E-PSE	-0.186	0.847		
PF	-0.239	0.289	0.793	
PD	-0.303	0.258	0.951	0.836

As shown in , each variable's square root (diagonal values) is greater than the correlation coefficients between variables (values below diagonal), indicating good discriminant validity.

4.4 Structural Model Analysis

This study used Partial Least Squares Structural Equation Modeling (PLS-SEM), which has fewer sample size requirements and no normal distribution requirements, making it more suitable for this research. WarpPLS software was used to test the structural equation model. The test showed overall fit parameters: APC = 0.267, ARS = 0.310, both significant at $p < 0.001$ level, and AVIF = 1.332, less than 3.3, which is ideal, indicating good model fit [57].

[Figure 2: see original paper] Structural Model Path Test Results (*** indicates $p < 0.001$)

As shown in [Figure 2: see original paper], the R^2 for privacy protection disengagement is 0.13, indicating that privacy protection self-efficacy can explain 13% of the variance in social network users' privacy protection disengagement behavior, suggesting that privacy protection self-efficacy plays a non-negligible role in social network users' privacy behaviors.

To verify the mediating role of privacy fatigue between privacy protection self-efficacy and privacy protection disengagement behavior, this study used a three-

step analysis method: (1) without the mediating variable, the independent variable has a significant effect on the dependent variable; (2) with the mediating variable, the independent variable has a significant effect on the mediating variable (if the independent variable still has a significant effect on the dependent variable at this time, it is partial mediation; if the effect is not significant, it is complete mediation) [58]. The analysis results are shown in [Figure 3: see original paper].

[Figure 3: see original paper] Mediation Effect Results (*** indicates $p < 0.001$)

As shown in [Figure 3: see original paper], after adding privacy fatigue, the R^2 for privacy protection disengagement became 0.39, indicating that the model with the mediating variable can explain 39% of the variance in social network users' privacy protection disengagement behavior, suggesting that privacy fatigue also plays an important role in social network users' privacy behaviors.

4.5 Research Results Analysis and Discussion

4.5.1 Research Results As shown in [Figure 2: see original paper] and [Figure 3: see original paper], except for H3 and H5, all other hypotheses passed (significance level $p < 0.05$), as shown in .

Hypotheses and Test Results

Hypothesis	Content	Result
H1	Privacy fatigue is positively correlated with privacy protection disengagement among social network users	Supported
H2	Internal privacy protection self-efficacy is negatively correlated with privacy fatigue among social network users	Supported
H3	External privacy protection self-efficacy is not correlated with privacy fatigue among social network users	Not supported (negative correlation)

Hypothesis	Content	Result
H4	Internal privacy protection self-efficacy is not directly correlated with privacy protection disengagement among social network users	Supported
H5	External privacy protection self-efficacy is positively correlated with privacy protection disengagement among social network users	Not supported

4.5.2 Analysis and Discussion Disengagement is a key outcome of fatigue [40], and this study reconfirms this conclusion in the context of social network users' privacy protection. According to construal level theory, social network users' cognition of privacy concerns is at a high construal level [59], while this distant future goal benefit cannot motivate those already fatigued by privacy protection behaviors [39], meaning users believe their privacy protection behaviors cannot bring sufficient benefits. Two possibilities may cause this cognition: First, frequent information leakage incidents [5-7] make users believe their attention to or measures for privacy protection are futile [8], as privacy protection behaviors cannot bring them more benefits or relief compensation. Second, underestimating data breach risks and insufficient understanding of privacy leakage hazards leads to inadequate negative emotional motivation. Research shows that users with higher privacy fatigue invest less effort in privacy decision-making [60], and this privacy fatigue has a particularly strong impact on disengagement behavior. Those fatigued by privacy decision-making are more likely to "stand by" when personal information is misused, consistent with this study's findings.

Privacy protection self-efficacy cannot directly influence social network users' privacy protection behaviors. Although self-efficacy has been proven to affect individuals' perceptions [43], behavioral intentions [57], and emotions [49], the existence of the "privacy paradox" phenomenon means that social network users' privacy concerns cannot predict their subsequent privacy disclosure or protection behaviors [59]. This study provides further evidence of the privacy paradox phenomenon from the side. H. Choi et al. [13] found that privacy fatigue weakens the negative relationship between privacy concerns and disclosure intentions. In the relationship between social network users' privacy protection self-efficacy and privacy protection disengagement behavior, privacy fatigue plays a similar

mediating role.

Second, privacy fatigue is an important process affecting users' decisions on whether to adopt privacy protection behaviors after cognitively assessing themselves and risk conditions, rather than merely a supplement to cognitive elements. As social networks become increasingly integrated into daily life, service providers have formulated more detailed terms and statements, giving users greater privacy control permissions (e.g., "visible to friends only," "show only last three days of moments"). However, not every user is willing to invest substantial time and energy to deeply understand these complex and obscure regulations and protocols or actively manage privacy when using social networks [37]. Instead, they continue using default settings, making these privacy statements seem like a form of "self-deception" by service providers that fails to truly gain user trust. Therefore, social network service providers should adopt more concise approaches, such as simplifying setup steps, pushing security reminder notifications, enabling privacy setting tutorials, displaying relevant risk warnings, improving privacy policy readability, using anthropomorphic communication [66], and changing default settings [67], to reduce user fatigue by lowering effort investment and increasing perceived benefits, thereby reducing users' privacy protection disengagement behaviors.

Finally, although the government has established general regulations in information privacy-related fields, discussions on online privacy issues from the consumer perspective should not stagnate. According to person-environment fit theory [68], when the mismatch between individuals' expectations and what the actual environment can provide exceeds the tolerance range, psychological stress increases. In social network environments, users hope their privacy will not be violated, yet privacy information leakage and misuse still occur. When this situation exceeds people's tolerance range, users experience privacy fatigue. Therefore, more discussion is needed on how to formulate policies to achieve acceptable privacy protection levels, and privacy protection self-efficacy provides a possible path for predicting privacy fatigue.

This study has certain limitations. First, although the model can explain 39% of privacy protection disengagement behavior and 23% of privacy fatigue variance, substantial variance remains unexplained. Excluding experimental errors, two possible reasons remain: (1) scale design issues—although measurement items were adapted from existing research, privacy protection self-efficacy research is currently immature, and its measurement items may require further refinement; (2) other factors may influence privacy fatigue and privacy protection disengagement behavior. Future research should focus on exploring these two aspects. Second, self-efficacy is unstable [69] and may be affected by temporary emotions. Future research may adopt multiple repeated survey methods [70] to minimize this error factor.

Conclusion and Outlook

This study analyzed the generation mechanism of social network users' privacy protection behaviors from a "disengagement" perspective, explored the concept and dimensions of privacy protection self-efficacy, and its role in social network users' privacy protection disengagement behavior.

This study provides important theoretical implications for better understanding online privacy behavior. First, current domestic research on privacy protection self-efficacy is scarce, and even fewer studies have examined its role and impact in social network users' related privacy behaviors. This study's primary contribution is distinguishing the conceptual dimensions of privacy protection self-efficacy and conducting empirical testing. Second, the study found that privacy protection self-efficacy has no direct effect on privacy protection disengagement behavior and requires privacy fatigue as a complete mediator. Enhancing social network users' confidence in their own abilities rather than external help can reduce their privacy fatigue, thereby reducing privacy protection disengagement behavior. Finally, given the existence of the privacy paradox in social networks, users' privacy concerns cannot serve as predictors of their privacy behaviors [62]. This study provides a possible research path for studying user privacy behavior.

In real life, privacy protection disengagement behavior does not mean consumers do not care about privacy issues. In fact, privacy concern is an important prerequisite for adopting information and communication technology (ICT) services [63], and most mobile internet users do not have high tolerance for privacy leakage [64]. As previous research on social network fatigue shows, social network users' fatigue intensifies their dissatisfaction with service providers [65]. Therefore, for social network service providers, enhancing users' internal privacy protection self-efficacy and reducing their external privacy protection self-efficacy may be a path to improve their usage intentions.

Since internal and external privacy protection self-efficacy have opposite effects on social network users' privacy fatigue, distinguishing privacy protection self-efficacy by source is necessary, which is fully reflected in subsequent predictive research on privacy fatigue. Enhancing social network users' internal privacy protection self-efficacy can reduce their privacy fatigue, consistent with relationships between self-efficacy and fatigue in other fields [48-49]. External privacy protection self-efficacy, conversely, exacerbates social network users' privacy fatigue. Research shows that attributing success to external contexts may weaken social network users' beliefs and perseverance in their personal privacy protection abilities. On the other hand, dependence on others often generates a social cost [61], which for social network users already unwilling to "waste" energy on privacy protection is undoubtedly "adding insult to injury."

References

[1] Chen D, Zhao H. Data security and privacy protection issues in cloud computing [C]//Proceedings of the 2012 International Conference on Computer Science

and Electronics Engineering. Washington, DC: IEEE Computer Society, 2012: 647-651.

[2] Pearsons. Taking account of privacy when designing cloud computing services [C]//Proceedings of the 2009 ICSE workshop on software engineering challenges of cloud computing. Washington, DC: IEEE Computer Society, 2009: 44-52.

[3] Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review [J]. MIS quarterly, 2011, 35(4): 989-1016.

[4] RiskBasedSecurity. Data breach quick view 2016 [EB/OL]. [2018-10-30] https://pages.riskbasedsecurity.com/2016-year-breach-quickview.

[5] GIGYA. The 2017 state of consumer privacy and trust [EB/OL]. [2018-10-30] http://www.199it.com/wp-content/uploads/2017/05/201704-Gigya-DS-Privacy_{{{Survey}}_{{Report}}}-web.pdf.

[6] Guo M. 2018 Kantar China Social Media Impact Report [EB/OL]. [2019-03-06] https://cn.kantar.com/media/social/2018/2018 年凯度中国社交媒体影响报告/.

[7] Anderson BB, Vance A, Kirwan CB, et al. From warning to wallpaper: why the brain habituates to security warnings and what can be done about it [J]. Journal of management information systems, 2016, 33(3): 713-743.

[8] Juhee K, Eric J. The market effect of healthcare security: do patients care about data breaches? [EB/OL]. [2018-10-30] https://www.econinfosec.org/archive/weis2015/papers/WEIS_{{

[9] Keith MJ, Maynes C, Lowry PB, et al. Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure [C]//International Conference on Information Systems (ICIS2014). Auckland: Social Science Electronic Publishing, 2014.

[10] Son JY, Kim SS. Internet users' information privacy-protective responses: a taxonomy and a nomological model [J]. MIS quarterly, 2008, 32(3): 503-529.

[11] Carver CS, Scheier MF, Weintraub JK. Assessing coping strategies: a theoretically based approach [J]. Journal of personality and social psychology, 1989, 56(2): 267-283.

[12] Kahn WA. Psychological conditions of personal engagement and disengagement at work [J]. Academy of management journal, 1990, 33(4): 692-724.

[13] Choi H, Park J, Jung Y. The role of privacy fatigue in online privacy behavior [J]. Computers in human behavior, 2018, 81(4): 42-51.

[14] Bien D, Torres AM. Social networking and online privacy: Facebook users' perceptions [J]. Irish journal of management, 2012, 31(2): 63-97.

[15] Pempek TA, Yermolayeva YA, Calvert SL. College students' social networking experiences on Facebook [J]. Journal of applied developmental psychology, 2009, 30(3): 227-238.

[16] Preibusch S, Krol K, Beresford AR. The privacy economics of voluntary over-disclosure in web forms [M]//Rainer B. The economics of information security and privacy. Berlin: Springer, 2013.

[17] Xu H, Dinev T, Smith HJ, et al. Information privacy concerns: linking individual perceptions with institutional privacy assurances [J]. Journal of the Association for Information Systems, 2011, 12(12): 798-824.

[18] Bandura A. Self-efficacy: toward a unifying theory of behavioral change [J]. Advances in behaviour research & therapy, 1977, 1(4): 139-161.

[19] Rifon NJ, LaRose R, Choi SM. Your privacy is sealed: effects of web privacy seals on trust and personal disclosures [J]. Journal of consumer affairs, 2005, 39(2): 339-362.

[20] Rhee HS, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior [J]. Computers & Security, 2009, 28(8): 816-826.

[21] Lee HH, Hill JT. Moderating effect of privacy self-efficacy on location-based mobile marketing [J]. International journal of mobile communications, 2013, 11(4): 330-350.

[22] LaRose R, Rifon NJ. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior [J]. Journal of consumer affairs, 2007, 41(1): 127-149.

[23] Bandura A. Social foundations of thought and action: a social cognitive theory [M]. Englewood Cliffs: Prentice-Hall, 1986.

[24] Sung HN, Jeong DY, Jeong YS, et al. The relationship among self-efficacy, social influence, performance expectancy, effort expectancy, and behavioral intention in mobile learning service [J]. International journal of u- and e-service, science and technology, 2015, 8(1): 1-8.

[25] Zhu YQ, Chen LY, Chen HG, et al. How does Internet information seeking help academic performance? The moderating and mediating roles of academic self-efficacy [J]. Computers & education, 2011, 57(4): 2476-2484.

[26] Lane J, Lane AM, Kyprianou A. Self-efficacy, self-esteem and their impact on academic performance [J]. Social behavior & personality, 2004, 32(3): 247-256.

[27] Youn S. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents [J]. Journal of consumer affairs, 2009, 43(3): 389-418.

[28] Rotter JB. Generalized expectancies for internal versus external control of reinforcement [J]. Psychological monographs, 1965, 80(1): 1-28.

[29] Weiner B. An attributional theory of achievement motivation and emotion [J]. Psychological review, 1985, 92(4): 548.

[30] Thatcher JB, Zimmer JC, Gundlach MJ, et al. Internal and external dimensions of computer self-efficacy: an empirical examination [J]. IEEE transactions on engineering management, 2008, 55(4): 628-644.

[31] Zimmerman B. Self-efficacy and educational development [M]//Bandura A. Self-efficacy in changing societies. New York: Cambridge University Press, 1995: 202-231.

[32] Marakas GM, Johnson RD, Palmer JW. A theoretical model of differential social attributions toward computing technology: when the metaphor becomes the model [J]. International journal of human-computer studies, 2000, 52(4): 719-750.

[33] Vohs KD, Baumeister RF, Schmeichel BJ, et al. Making choices impairs subsequent self-control: a limited-resource account of decision making, self-regulation, and active initiative [J]. Journal of personality and social psychology, 2008, 94(5): 883-898.

[34] Acquisti A, Telang R, Friedman A. Is there a cost to privacy breaches? An event study [C]//Twenty Seventh International Conference on Information Systems. Milwaukee: WI, 2006: 1563-1580.

[35] Levav J, Heitmann M, Herrmann A, et al. Order in product customization decisions: evidence from field experiments [J]. Journal of political economy, 2010, 118(2): 274-299.

[36] Schermer BW, Custers B, Simone VD. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection [J]. Ethics and information technology, 2014, 16(2): 171-182.

[37] Zhu H, Zhang MX, Lu YH. Empirical study on social media users' willingness to read privacy policies [J]. Journal of the China Society for Scientific and Technical Information, 2018, 37(4): 362-371.

[38] Ax S, Gregg VH, Jones D. Coping and illness cognitions: chronic fatigue syndrome [J]. Clinical psychology review, 2001, 21(2): 161-182.

[39] Hopstaken JF, Linden DV, Bakker AB, et al. A multifaceted investigation of the link between mental fatigue and task disengagement [J]. Psychophysiology, 2015, 52(3): 305-315.

[40] Demerouti E, Mostert K, Bakker AB. Burnout and work engagement: a thorough investigation of the independence of both constructs [J]. Journal of occupational health psychology, 2010, 15(3): 209-222.

[41] Bakker A, Demerouti E, Verbeke W. Using the job demands-resources model to predict burnout and performance [J]. Human resource management, 2004, 43(1): 83-104.

[42] Igbaria M, Iivari J. The effects of self-efficacy on computer usage [J]. Omega, 1995, 23(6): 587-605.

[43] Compeau D, Higgins CA, Huff S. Social cognitive theory and individual reactions to computing technology: a longitudinal study [J]. MIS quarterly, 1999, 23(2): 145-158.

[44] Chen H, Li WL. Research on information security protection behavior based on emotion mediation [J]. Science research management, 2018, 39(6): 48-56.

[45] Morin L, Latham G. The effect of mental practice and goal setting as a transfer of training intervention on supervisors' self-efficacy and communication skills: an exploratory study [J]. Applied psychology, 2000, 49(49): 566-578.

[46] Schaefers KG, Epperson DL, Nauta MM. Women's career development: can theoretically derived variables predict persistence in engineering majors? [J]. Journal of counseling psychology, 1997, 44(2): 173-183.

[47] Bandura A, Wood R. Effect of perceived controllability and performance standards on self-regulation of complex decision making [J]. Journal of personality & social psychology, 1989, 56(5): 805-814.

[48] Johansson AC, Brink E, Cliffordson C, et al. The function of fatigue and illness perceptions as mediators between self-efficacy and health-related quality of life during the first year after surgery in persons treated for colorectal cancer [J]. Journal of clinical nursing, 2018, 27(7): 1537-1548.

[49] Zuckerman M. Attribution of success and failure revisited: or the motivational bias is alive and well in attribution theory [J]. Journal of personality, 1979, 47(2): 245-287.

[50] Bandura A. Self-efficacy: the exercise of control [J]. Journal of cognitive psychotherapy, 1997, 13(2): 158-166.

[51] Cho H, Lee JS, Chung S. Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience [J]. Computers in human behavior, 2010, 26(5): 987-995.

[52] Baek YM, Kim EM, Bae Y. My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns [J]. Computers in human behavior, 2014, 31(31): 48-56.

[53] Jrn K, Dickson PR. How believing in ourselves increases risk taking: perceived self-efficacy and opportunity recognition [J]. Decision sciences, 1994, 25(3): 385-400.

[54] Milne GR, Labrecque LI, Cromer C. Toward an understanding of the online consumer's risky behavior and protection practices [J]. Journal of consumer affairs, 2009, 43(3): 449-473.

[55] Barth S, De Jong M. The privacy paradox: investigating discrepancies between expressed privacy concerns and actual online behavior [J]. Computers & security, 2017, 64(1): 122-134.

[56] Kokolakis S. Privacy attitudes and privacy behavior: a review of current research on the privacy paradox phenomenon [J]. Computers & security, 2017, 64(1): 122-134.

[57] WarpPLS 5.0 User Manual [EB/OL]. [2018-11-23] http://cits.tamiu.edu/WarpPLS/UserManual_{v_5}0.p

[58] Baron RM, Kenny DA. The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations [J]. Journal of personality and social psychology, 1986, 51(6): 1173-1182.

[59] Li H, Yu L, Xu YM, et al. Research on social network privacy paradox from the perspective of construal level theory [J]. Journal of the China Society for Scientific and Technical Information, 2018, 37(1): 1-13.

[60] Stanton B, Theofanos MF, Prettyman SS, et al. Security fatigue [J]. IT professional, 2016, 18(5): 26-32.

[61] Morrison EW. Newcomer information seeking: exploring types, modes, sources, and outcomes [J]. Academy of management journal, 1993, 36(3): 557-589.

[62] Xie XZ, Cai NZ, Huang ZM, et al. Preliminary exploration of factors influencing social media users' privacy paradox behavior [J]. Library and information service, 2018, 62(18): 55-63.

[63] Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions [J]. Information systems research, 2006, 17(1): 61-80.

[64] Li R, Zhang RJ, Li WL, et al. Measurement method for privacy leakage tolerance in mobile internet environment [J]. Management review, 2016, 28(7): 102-111.

[65] Zhang S, Zhao L, Lu Y, et al. Do you get tired of socializing? An empirical explanation of discontinuous usage behavior in social network services [J]. Information & management, 2016, 53(7): 904-914.

[66] Zeng FE, Zou Z, Tao R. Will personalized marketing necessarily trigger privacy concerns? Based on the perspective of anthropomorphic communication [J]. Nankai business review, 2018, 21(5): 83-92.

[67] Shen HZ, Tang XT, Zhou Y. Usability research on privacy protection functions of mobile social media in China [J]. Library and information service, 2017, 61(4): 23-30.

[68] Spokane AR, Meir EI, Catalano M. Person-Environment congruence and Holland's theory: a review and reconsideration [J]. Journal of vocational behavior, 2000, 57(2): 137-187.

[69] Weiner B. Human motivation [M]. New York: Springer, 1985.

[70] Chen IS. Computer self-efficacy, learning performance, and the mediating role of learning engagement [J]. Computers in human behavior, 2017, 72(7): 362-370.

Author Contributions

Xu Yiming: Research design, literature review, initial draft writing
Li He: Research design, initial draft revision
Yu Lu: Data collection and organization

Research on the Influence of Self-efficacy of Privacy Protection on Privacy Behaviors of Social Network Users

Xu Yiming, Li He, Yu Lu
School of Management, Jilin University, Changchun 130022

Abstract: [Purpose/significance] With the frequent occurrence of data leakage events, more and more social network users have questioned the effectiveness of their privacy protection behaviors and even abandoned protection strategies for privacy information. This paper attempts to explore the reasons why social network users give up privacy protection from the perspective of privacy protection self-efficacy. [Method/process] By sorting out relevant literature on self-efficacy, privacy fatigue was introduced as an intermediary variable, a structural equation model was established, and data were obtained through questionnaire surveys for analysis. [Result/conclusion] The privacy protection self-efficacy of social network users cannot directly influence their privacy protection disengagement behavior and needs to exert indirect influence through the complete mediating variable of privacy fatigue. Different sources of privacy protection self-efficacy have different effects.

Keywords: privacy protection; self-efficacy; privacy fatigue; disengagement; privacy behavior

Note: Figure translations are in progress. See original paper for figures.