

The factors influencing individual's behavior on privacy protection

SHENG-FEI HSU, DONG-HER SHIH
Department of Information Management
National Yunlin University of Science & Technology
123, University Road, Douliu, Yunlin
TAIWAN
g9320803@yuntech.edu.tw

Abstract: Individual's behavior on privacy protecting is affected by not only the personal psychological factors, but also the external influences. However, the latter was always ignored in previous researches. For investigating how the external as well as internal factors simultaneously affected one's privacy concern on privacy protection and restrained related behavior, this study applied perceived behavior control to modifying previous privacy model. In addition, a hypothesized model proposed to interpret how the related factors influenced individual's behavior on privacy protection. The result of this study also indicated the significant relationships between personal privacy perception and perceived behavioral control.

Key-Words:- Privacy concern, Perceived privacy, Trust, Perceived behavioral control, Behavior on privacy-protecting, Theory of planned behavior.

1 Introduction

Over the past decade, the Internet has become an important and ubiquitous feature in the developed world. The increasing use of the Internet, together with rapid advances in technology, has changed the way in which information about users was gathered, stored and exchanged. Accordingly, concerns about the online privacy have grown in importance [1]. Although, previous research has studied related issues from different perspectives, such as consumers' concerns about information privacy [2], consumer's willingness to provide personal information [3], the effect of trust (in the organization) on customers' willingness to provide information [4], the contents of privacy disclosures [5], and legal and ethical issues associated with

privacy [6]. Little study conducted directly with the individuals' perspectives on privacy protection and related external influence in psychological setting. For filling this gap, authors present a research that examines the links between people's subjective cognition and attitude on individuals' behavior about privacy protection, and the influence from perceived behavioral control. Research also proposes a hypothesized model to verify and interpret the results.

2 Literature review

The use of new technology, particularly the Internet, increasingly required people to disclose personal information online for various reasons. These

technological developments have raised a number of privacy concerns [7]. However, privacy was a changeable concept that encompassed a variety of meanings [8]. Technology and the Internet posed unique privacy issues that differed from those previously addressed by privacy research. For instance, in e-commerce, users might be concerned about whether the information about their purchases was stored, or sold to the third parties who would then send them unwanted mail. In particular, the more traditional ways of understanding and defining privacy did not account for the unique problems technology has introduced [9]. Obviously, technology created privacy issues that appeared to fall outside the bounds of traditional analysis [10].

Central to the definition of privacy was the issue of privacy concern [11]. Over the past decade, the concept of privacy concern has been regularly applied to the Internet, and some reports revealed that the offline privacy concerns appeared to be magnified online [1]. Previous studies have consistently indicated that the overwhelming majority of people were 'concerned' or 'very concerned' about threats to their privacy while online, and were willing to act to protect it [12]. In addition, similar issues were discussed from other perspectives in the parallel event, such as examining consumers' information privacy concerns [13][14][15], the self-disclose and privacy in new communication technology [16][17], privacy within social networking sites [18], and the effect of cultural values on an individual information privacy concerns [19][20].

Furthermore, the theory of planned behavior (TPB) [21] has emerged as a promising framework for the study of human behavior, including technology adoption and usage. In which, perceived behavioral control, as one of the three

main constructs, had influence on people's intention and behavior. Conceptually, perceived behavioral control reflected barriers toward performing a behavior, and indicated an external aspect of control [22]. Prior research also defined perceived behavioral control as the ability to control over difficult situation and barrier [23]. The above review presented the focuses at which previous studies aimed, it also involved perceived behavioral control, which was used to modify the prior researches in this study.

3 Method

3.1 Theoretical model

Leading scholars proposed four factors to illustrate the personal perception on self-disclosure; they were privacy concern, perceived privacy, trust, and past privacy behavior [24]. Privacy concern represented personal attitude; and perceived privacy indicated subjective cognition; trust was the willingness to be vulnerable, based on positive expectations about the actions of others [25]; and past privacy behavior showed personal experience. Although, these researches focused on predicting personal self-disclose or non-disclose online, its model and related constructs provided a worthwhile reference on this research.

3.2 Research model and hypotheses

While examining the user's behavior on protecting privacy, perceived privacy and privacy concern were two indispensable components. Both of them provided two significant pathways to indicate situational and dispositional aspects in psychological setting. However, influences from external factors should not ignore as well. While considering external influence on individuals' behavior, perceived behavioral control, deriving

from theory of planned behavior [26], played a significant role in predicting a person's behavioral intention or behavior directly. It reflected beliefs regarding the access to resources and opportunities needed to perform a behavior, in other words, it referred to people's perceptions of their ability to perform a given behavior.

Perceived privacy indicated the subjective cognition over controlling information disclosing, it presented that user's control on providing information online based on the reliability of the websites. For considering reliability, user would ponder over several related factors, such as the reputation of the company, necessity, and benefits.

In addition, trust was the willingness to be vulnerable, based on positive expectations about the actions of others [25], it was also defined as expectancy held by individuals or groups that the word, promise, verbal, or written statement of another could be relied on. On the internet, privacy policies of websites contained descriptions of their privacy practices for the online collection, use, and dissemination of personal information. Users would like to criticize these privacy policies before conducting technical protection.

Further, individuals' behavior on privacy protection was one of the main topics in this research. The Internet was neither owned nor controlled by any one company or any one government, but an electronic infrastructure built on open standards. These open standards allowed for connectivity and communication to occur without regard to domestic borders or proprietary jurisdictions. In other words, it would be easy to take the position that with or without the user's consent. Moreover, some companies used electric data techniques to capture personal data without permit, such as cookie, spy ware. That made people concern about privacy invasions and would try to

take protection. Therefore, the first two hypotheses were proposed.

H1: Users' perceived privacy had positive effect on trust.

H2: Trust had positive effect on users' behavior on privacy protection.

Privacy concern was one of important factors which presented personal attitude on controlling cognitive and affective inputs and outputs, forming values, as well as the right to determine with whom and under what circumstances thoughts would be shared or intimate information revealed [7]. Further, privacy concern was a subjective measure – one that varied from individual to individual based on person's own perception and values. Prior surveys confirmed that Internet users generally felt differently about the disclosure of different types of information. They were usually quite willing to disclose basic demographic and lifestyle information as well as personal tastes and hobbies. They were slightly less willing to disclose details about their Internet behavior and purchases, followed by more extended demographic information. Financial information, contact information, and specifically credit card and social security numbers raised the highest privacy concerns.

Besides users' concern for privacy, individuals' Internet experience and past online information disclosure were also likely to influence their disclosure to commercial Web sites. Based on the truism that the best predictor of future behavior was past behavior, prior disclosure of personal information was likely to affect later disclosure. In other words, past privacy behavior showed experiences related with personal privacy concern, and would treat as a reference while disclosing personal privacy. Then, another two hypotheses posited.

H3: Privacy concern had positive effect on users'

past privacy behavior.

H4: Individual's past privacy behavior had positive effect on behavior on privacy protection.

Perceived behavioral control showed the perceptions of how easy or difficult it would be to take a particular action and recognized that behavior was not always under voluntary control. That meant that sufficient knowledge and experience would increase user's ability on controlling the influences from external environment. Therefore, the fifth hypothesis derived.

H5: Perceived behavioral control had positive effect on individual's behavior on privacy protection.

3.3 Measures

For verifying the hypotheses, the questionnaire contained measures of behavior on privacy protection, perceived privacy, trust, privacy concerns, past privacy behavior, and perceived behavioral control. The survey items provided in Table 1, and all items were answered using a five-point Likert scale (1= completely disagree, 3 = neutral, 5 = completely agree). Further, the participants filled out the questionnaire were undergraduate students in Taiwan (N=162), 45 were women and 117 were men. Seventy-eight students were day division while eighty-four joined evening division. The average age of the students in day division was 20 (SD=1.00); 71 were men and seven were women. The average age of the students in evening division was slightly higher (M=30.9; SD=7.96), and there were fewer men and more women than in the day division sample (46 men and 38 women in the evening division sample). Surveys administered in class. In addition, one pretest on a convenience sample of 34 university

students was conducted to check whether the questionnaire could work as intended.

4 Analysis

SPSS was utilized for all analyses in this research. Besides descriptive analysis for demographics, factor analysis applied to measuring validity and extracting factors. And Chi-square good-of-fit test was conducted to see if the sample came from the population with the claimed distribution. The null hypothesis would be rejected at 5% statistical significance level ($p < .05$), which was a commonly used procedure for taking into account the probability of making one or more Type I error. Moreover, correlation analysis used to measure the correlation between related constructs. In variance analysis, F test was used to test the significance of a series of regression coefficients. Furthermore, a series of multiple regression analysis applied to analyzing the relationships between dependent and independent. Then, path analysis, a statistical method of finding cause/effect relationships, also an extension of the regression model, applied to testing the fit of the correlation matrix against two or more causal models that were being compared.

5 Result

In research, for evaluating whether variables were uniform and could be clustered as a construct, tests of KMO (Kaiser-Meyer- Olkin measure of sampling adequacy) was utilized to test the suitability. And Cronbach's alpha, measuring the level of consistency as reliability analysis, was also applied. It showed that both of them were greater than 0.60 that indicated acceptable. Further, for examining the relationships between related constructs, correlation analysis applied on this

research. The most common measure was the Pearson's correlation coefficient, which reflected the degree of liner relationship between two related constructs. It indicated that all the correlations in

this research between related constructs had positive significant correlation ($p=.000<.01$) (Table 2).

Table 1: summary of items of construct

Construct	Item	Factor loading
Perceived privacy	The reputation of the company/person requesting the information	.914
	Trusting the company/person requesting the information	.888
	The need for the information being requested	.885
	The benefits of disclosing the information requested	.870
Trust	The design of the webpage	.451
	The inclusion of a privacy policy on the webpage	.922
	The content of the privacy policy on the webpage	.929
Privacy concern	Individual's concern about his/her privacy while using the internet.	.768
	Individual's concern about online organizations not being who they claim they are.	.823
	Individual's concern about providing too much personal information when registering or making online purchases.	.710
	Individual's concern about online identity theft.	.816
	Individual's concern about people online not being who they say they are.	.802
	Individual's concern about people you do not know obtaining personal information about you from your online activities.	.760
Past privacy behavior	Shredding/burning your personal documents when you are disposing of them	.569
	Hiding bank card PIN number when using cash machines/making purchases	.649
	Only registering for websites with a privacy policy	.766
	Reading a website's privacy policy before registering for you information	.849
	Looking for a privacy certification on a website before registering information	.809
	Reading license agreements fully before agreeing to them	.728
Perceived behavioral control	Accessing personal medical records without permit.	.925
	An email sending someone may be read by others.	.910
	An email sending someone may be inappropriately forwarded to others.	.904
	An email sending someone may be printed out in a place where others could see it.	.665
Behavior on privacy protection	Removing cookie.	.672
	Using a pop up window blocker.	.709
	Checking computer for spy ware.	.731
	Clearing browser history regularly.	.723
	Blocking messages/email from someone you do not want to here from.	.695

Table 2: Correlations matrix of constructs

		PP	TR	PC	PRB	PBC	BE
Perceived privacy (PP)	Pearson Correlation (r)	1	.436	.315	.341	.171	.297
	Sig. (2-tailed)		.000	.000	.000	.000	.000
	N		162	162	162	162	162
Trust (TR)	Pearson Correlation (r)		1	.405	.483	.365	.202
	Sig. (2-tailed)			.000	.000	.000	.000
	N			162	162	162	162
Privacy concern (PC)	Pearson Correlation (r)			1	.487	.596	.289
	Sig. (2-tailed)				.000	.000	.000
	N				162	162	162
Past privacy behavior (PRB)	Pearson Correlation (r)				1	.333	.361
	Sig. (2-tailed)					.000	.000
	N					162	162
Perceived behavioral control (PBC)	Pearson Correlation (r)					1	.212
	Sig. (2-tailed)						.000
	N						162
Behavior on protecting privacy (BE)	Pearson Correlation (r)						1
	Sig. (2-tailed)						
	N						

** Correlation is significant at the 0.01 level (2-tailed).

On the procedure of regression analysis, both R^2 and F test of related constructs were measured and showed significant (Table 3). Moreover, the standard coefficient of β distribution applied to construct a final hypothesized model and verify its adequacy (Figure 1). It indicated that users' perceived privacy had positive direct effect on trust ($\beta=.436$, $p=.000<.001$), but had insignificant positive indirect effect on behavior on protecting privacy while mediated through trust ($\beta=.043$, $p=.379>.05$). Even so, analysis showed that perceived privacy had significant positive direct effect on behavior on protecting privacy ($\beta=.190$, $p=.000<.001$). Further, privacy concern had positive direct effect on past privacy behavior ($\beta=.487$, $p=.000<.001$), and it had positive indicate effect on behavior on protecting

privacy ($\beta=.266$, $p=.000<.001$), mediated through past privacy behavior. Moreover, perceived behavioral control had positive direct effort on behavior on protecting privacy ($\beta=.091$, $p=.028<.05$). Therefore, all the hypotheses were verified except hypothesis H2, and a significant new path from perceived privacy to behavior on protecting-privacy appeared.

6 Discussion and implication

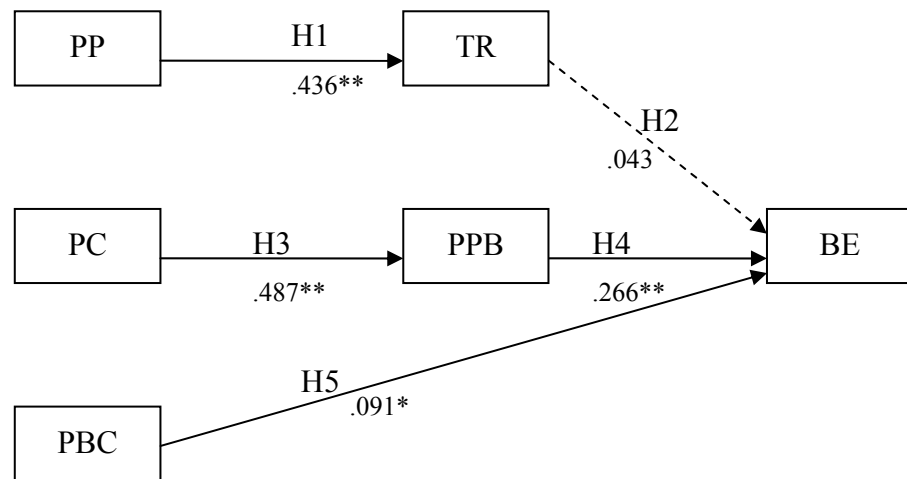
User's behavior on protecting privacy is influenced by two kinds of factors, internal and external. For internal factors, previous research provided two pathways on the privacy-trust-disclose model to describe the interaction and dispositional pathway

presented user's belief on privacy protection [7]. On the other hand, while observing the questions about perceived privacy in the questionnaire and its further link with trust, it reveals user's subjective cognition on the related criteria, such as reputation, as well as the evaluation of necessity and benefits. Subjective perceived privacy may be affected by experts' suggestions, learning in school, and experiences from peers. Through this conceptual development, all of these form user's perception on evaluating trustworthiness of websites and embodies the concept of trust. This development verifies the causal model in the hypothesis H1. In other words,

situational pathway significantly indicates normative attribution. However, trust presents individual's perception on uncertainty and risk, as well as the willingness to engage in related behavior, but has little casual relationship with behavior on protecting privacy, which focused on technical manipulation. Therefore, hypothesis H2 was rejected ($\beta=.043$, $p=.379>.05$). Nevertheless, research shows that users' perceived privacy would prompt them to conduct some technical protection to shield from inadequate access on personal information. In other words, users' perceived behavior has significant direct effect on behavior on protecting privacy.

Table 3: Model summary for hypothesized model

Model 1	R	R ²	F value	Sig.
Dependent variable : Trust (TR)	.436	.190	128.801	.000
Predictor : (Constant), Perceived privacy (PP)				
Dependent variable : Past privacy behavior (PPB)	.487	.237	170.304	.000
Predictor : (Constant), Privacy concern (PC)				
Dependent variable : BE (SD)	.415	.172	37.865	.000
Predictors : (Constant), TR, PPB, PBC.				



* p<.05; **p<.001

Figure 1. Path chart of hypothesized model

Another pathway involves in the internal factors of this hypothesized model is dispositional pathway which is derived from privacy concern. Although privacy concern is not clearly established so far [27], previous studies revealed that privacy concern, affected by secondary use of information control [28], was a function of the cumulative information rather than just the concern from the individual pieces of information. [29]. Further, privacy concern indicates individual's expectation on controlling personal information and its further application. These attempts influence individual's action, and can be examined on personal past behavior, such as shredding personal document, or hiding bankcard PIN number. Obviously, these descriptions verify the causal model in the hypothesis H3 that the privacy concern had a positive direct effect on past privacy behavior. Further, mediating through individuals' past privacy behavior, user's privacy concern indicated a positive indirect effect on behavior on protecting information.

Besides, the external factor also releases crucial influences on personal privacy management. In the hypothesized model, perceived behavioral control is defined as one's assessment of how hard or easy it is to carry out a given behavior. In other words, environment one involved will affect his/her behavior. Previous studies showed that personal ability on controlling and managing personal information was limited under several situations, such as interferences from spy ware, identity theft, as well as phishing, and cookies. For shielding from these malicious invasions, many people use technical protection or skill to avoid these annoying disturbances. Therefore, hypothesis H5 was verified that individuals' perceived behavioral control had positive direct effect on behavior on protecting privacy. This situation presented the external

influences on person's behavior, and individual's ability to control or mitigate its influence.

This study also has several limitations. First, this study focused on personal privacy protection and ignored organization's situation, such as companies, who also suffered privacy problems. Second, the hypothesized model might have excluded some other constructs from the study. Other constructs, such as the ability on monitoring malicious invasion and risk assessment, might influence individual's behavior on protecting information online. Hence, future research may extend the study to cover other groups and add additional constructs to the model.

Although current privacy researches tend to focus on the issues about the trust in B-to-C relationship, and privacy management on computer-mediated communication, the vision on personal protecting online privacy in psychological setting, as well as its further development is still blurred and worthy to explore. For investigating the factors of protecting online privacy and understanding the interactions, this study examined the influences on personal protecting privacy not only from the aspects of individual's internal cognitive assessment, but also considered the interferences from external environment. Research show that individual's behavior is mainly based on subjective cognition and perception on privacy, but the uncertainty exists in the external environment may interfered one's behavior.

7 Conclusions

Research on the factors influencing individual's behavior on privacy-protecting aimed at reconciling the goals and methods of privacy-trust-disclose model and perceived behavioral control, and at analyzing the interaction within perceived privacy, privacy concern, as well

as perceived behavioral control, and it further development on behavior. Several contributions released in this article. Firstly, it led the concept of perceived behavioral control into the behavior on privacy protection and proved its influences. Second, it provided another vision to take into account the external influences on individual's perception and related attitude. Third, it embedded the construct of perceived behavioral control to expand the view on privacy protection. These constructs and the relationships between them would serve as a basis for future empirical studies on related issues.

References:

- [1] Painea, Ulf-Dietrich Reipsb, Stefan Stiegerc, Adam Joinsona, Tom Buchanan, "Internet users' perceptions of 'privacy concerns' and 'privacy actions'", *Int. J. Human-Computer studies*, Vol.65, 2007, pp.526–536.
- [2] Chang Liu, Jack T. Marchewka, June Lu, Chun-Sheng Yu, Beyond concern—a privacy-trust-behavioral intention model of electronic commerce, *Information & Management*, Vol.42, 2005, pp.289–304.
- [3] Yue Pan, George M. Zinkhan, Exploring the impact of online privacy disclosures on consumer trust, *Journal of Retailing*, Vol.82, (4), 2006, pp.331–338.
- [4] Schoenbachler, Denise D. and Geoffrey L. Gordon, Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing, *Journal of Interactive Marketing*, Vol.16, (3), 2002, pp.2–16.
- [5] Miyazaki, AnthonyD. and Ana. Fernandez, Internet Privacy and Security: An Examination of Online Retailer Disclosures, *Journal of Public Policy & Marketing*, Vol.19, 2002, pp.54–61.
- [6] R.R. Rowlingson, Marrying privacy law to information security, *Computer Fraud & Security*, Issue 8, August 2006, pp.4-6.
- [7] Joinson, A. N., Paine, C., Reips, U.-D. and Buchanan, T. , Privacy and Trust: The role of situational and dispositional variables in online disclosure, *Proc. of Privacy, Trust, and Identity*. Issues for Ambient Intelligence Workshop, 2006, pp.1-6.
- [8] Clarke R., Internet Privacy Concerns Confirm the Case for Intervention, *Communications of the ACM*, Vol.42 (2), 1999, pp.60-67.
- [9] Solove D.J., The Digital Person. *Technology and Privacy in the Information Age*, NYU Press, New York 2004.
- [10] Austin L., Privacy and the question of technology, *Law and Philosophy*, Vol.22, 2003, pp.119–166.
- [11] Westin, A., Privacy and Freedom, Atheneum, New York, 1967.
- [12] Electronic Privacy Information Center, Public Opinion on Privacy. Available from <http://epic.org/privacy/survey/>, accessed on 20, March, 2009.
- [13] Y. Chan, Culnan, M., Greenaway, K., Laden, G., Levin, T., Smith, H. J., Information Privacy: Management, Marketplace, and Legal Challenges, *Communications of the Association for Information Systems*, Vol. 16, 2005, pp.270-298.
- [14] M. Arami, Treiblmaier, H., Pinterits, A., Madlberger, M., Information Privacy Concerns and E-Commerce: An Empirical Investigation, in *Proceeding of Tenth Americas Conference on Information*

- Systems*, New York, New York., 2004, pp.1178-1189.
- [15] K. Chen, Rea Jr., A. I., Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques, *Journal of Computer Information Systems*, vol. Summer, 2004, pp.85-92.
- [16] Malhotra, N.K., Kim, S., Agarwal, J., Internet users' information privacy concerns, IUIPC: the construct, the scale and a causal model, *Information Systems Research* Vol.15, 2004, pp.336–355.
- [17] Tidwell, L. C., &Walther, J. B., Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time, *Human Communication Research*, Vol.28, 2002, pp.317–348
- [18] Dwyer, C., Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study, *Proceedings of the 40th Hawaii International Conference on System Sciences* (HICSS), Hawaii, 2007.
- [19] Dinev, t., Hart, P., Internet privacy concerns and their antecedents - measurement validity and a regression model, *Behaviour & Information Technology*, Vol. 23, 2004, pp.413-422.
- [20] C. Hsu, Privacy concerns, privacy practices and web site categories – Toward a situational paradigm, *Online Information Review*, Vol. 30, 2006, pp.569-585.
- [21] Ajzen, I., Perceived behavioural control, self-efficacy, locus of control, and the theory of planned behaviour, *Journal of Applied Social Psychology*, Vol.32, 2002, pp.1–20.
- [22] Terry, D.J. and O'Leary, J.E., The Theory of Planned Behaviour: The effects of perceived behavioural control and self-efficacy, *British Journal of Social Psychology*, Vol.34, 1995, pp.403-4 15.
- [23] Hagger, M., Chatzisarantis, N., and Biddle, S., The influence of self-efficacy and past behaviour on the physical activity intentions of young people, *Journal of Sports Sciences*, Vol.19, 2001, pp.711-725.
- [24] Adam Joinson, Privacy and Self-Disclosure Online, *ESRC End of Award Report*, RES-341-25-0011. Swindon: ESRC, 2007.
- [25] Bos, N., Olson, J. S., Gergle, D., Olson, G. M., & Wright, Z., Rich media helps trust development, *Proceedings of CHI 2002*, 135–140. New York: ACM Press, 2002.
- [26] Ajzen, I. & Fishbein, M., *Understanding attitudes and predicting social behaviour*, Englewood Cliffs, NJ: Prentice-Hall, 1980.
- [27] Alfred Kobsa, Privacy-Enhanced Personalization, *Communications of the ACM*, 50 (8), 2007, 24-33.
- [28] DL Hoffman, TP Novak, MA Peralta, Information Privacy in the Marketplace: Implications for the Commercial Uses of Anonymity on the Web, *The Information Society*, 1999
- [29] Chellappa, Rammnath K. and Raymond Sin, Online personalization versus privacy concerns: modelling the flip sides of the same coin, *ebizlab* (Marshall School of Business, USC), 2001'