2009

Raising Students' Concept in Protecting Information Privacy through Information Ethics Education

Cathy S. Lin
National University of Kaohsiung, cathy@nuk.edu.tw

Sheng Wu
Southern Taiwan University of Technology, shengwu@mail.stut.edu.tw

Raising Students' Concept in Protecting Information Privacy through Information Ethics Education

Cathy S. Lin
National University of Kaohsiung
cathy@nuk.edu.tw

Sheng Wu
Southern Taiwan University
shengwu@mail.stut.edu.tw

ABSTRACT

The concept of privacy in Chinese context is a fragile perception. Under such a culture environment, the awareness of right of privacy raises late; therefore, it is of necessary raising people the concept of information privacy. To reach this purpose, this study adopts the theory of self-efficacy to examine factors that influence decisions related to information privacy. Further, a longitudinal model is explored whether information ethics education plays a role influencing students' concept in protecting information privacy.

A survey with senior-level undergraduate students is conducted to test the hypothesized model. The findings exhibit an important insight that through information ethics education, students demonstrate a significant change in their confidence of privacy self-efficacy; the increase of this concept noteworthy changes their behavior concerning information privacy protection. Finally, discussions and conclusions are discussed.

Keywords

Privacy, Self-Efficacy, Information Ethics Education, IS Curriculum.

INTRODUCTION

As Chinese Proverb says, "water, capable of carrying vessels, is also capable of getting vessels capsized", the information technology (IT) is right the case. The privacy concerns now re-emerge right because the public perceives a threat from new information technologies that are equipped with enhanced capabilities for surveillance, storage, retrieval, and transmission of personal information (Clarke, 1988; Gentile & Sviokla, 1990; Mason, 1986; Miller, 1971; Westin, 1967). The concept of privacy in Chinese context is a fragile perception. The privacy in traditional Chinese culture is treated as a kind of right that the authority owns; those who are disadvantaged minority often have to sacrifice their privacy in order to abide by the authority. Under such circumstances, the concept concerning the right of privacy raises late.

While the world relies more on IT now than ever before, it is of necessary raising people the concept of information privacy. Especially when those students who major in information systems, they imperatively have an obligation understanding the responsibility that goes with there IS profession. Their values concerning information privacy will affect how they write programs, view privacy and security issues, and handle critical software. To reach this purpose, information ethics education is described as the ideal way to teach information about correct usage to students. In this study, we focus on raising one's privacy self-efficacy through information ethics education; it is expected that students can exercise substantial personal control over educational learning about the recognition of appropriate behavior toward information privacy. Therefore, this study adopts the theory of self-efficacy from social-psychology perspective to see the variation in this concept. This study focus on the crucial construct of privacy self-efficacy to examine factors that influence decisions related to information privacy. In this model, attitude toward privacy protection, privacy self-efficacy, and privacy intention are identified and incorporated. What is more, we are interested in whether information ethics education can significantly build up students' attitude toward privacy protection, privacy self-efficacy, privacy intention and behavior. It is helpful for educators to incorporate consciousness of social and ethical information issues into IS curriculum. Altogether, two research questions are listed:

RQ1: The constructs of attitude toward privacy protection and privacy self-efficacy are hypothesized to have a significant role as direct determinants of privacy intention and behavior.

RQ2: There have significant differences between pre-education and post-education students in the relationships that the effects of attitude toward privacy protection, privacy self-efficacy, and privacy intention have on behavior.

Theory of Self-Efficacy

According to the theory of self-efficacy, the concept self-efficacy is defined as the belief that one has the capability to execute a particular action, which is seen a major determinant of people's choices of activities, how much effort they will expend, and how long they will sustain the effort in dealing with stressful situations (Bandura, 1977, 1986). That is, individuals who have a stronger perceived self-regulatory efficacy will tend to behave well self-controlling efforts and will be able to better resist social pressure. On the contrast, those who have a low sense of self-regulatory efficacy ones will heighten vulnerability to social pressures for transgressive conduct (Bandura, 1991).

The robustness of self-efficacy has been established through many applications and replications across a broad range of behavioral domains including information systems (Bandura, 1997; Compeau and Higgins, 1995; Latham and Frayne, 1989; Marakas, et al., 1998). For example, several researchers in IS-related studies have focused their attention on how computer self-efficacy expectation may impact decisions concerning technology acceptance and usage (Compeau and Higgins, 1995; Gist and Mitchell, 1992; Hill et al, 1987; Henry and Stone, 1997). For the reasons given above, this research relies on the Bandura's self-efficacy theory to address the question of whether strengthen of perceived self-efficacy will increase IS students' capability concerning protecting information privacy.

RESEARCH MODEL

In this study, the perceived self-efficacy is included as an attempt to strengthen the individual's behavioral intention behaviors where volition or autonomous control is limited. The importance of self-efficacy as a predictor of behavior is greater in activities where the person has only variable or limited control over the behavior (Ajzen, 2002). Moreover, Ajzen & Fishbein (1980) showed that attitudes and intentions are the best predictors of specific behaviors. Therefore, this research posits that attitude toward privacy protection and the privacy self-efficacy are critical factors essential to the behavioral intention (see Figure 1).

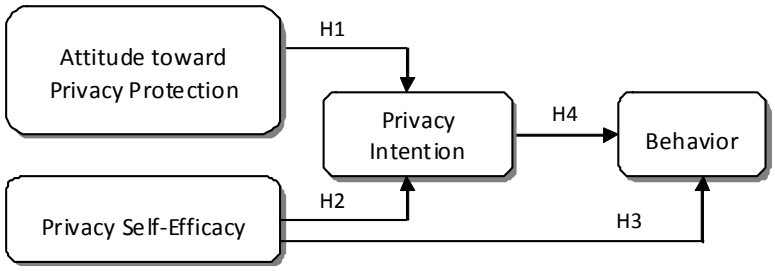

Figure 1. Research Model

In this model, four basic hypotheses are examined:

[H1] There is a positive relationship between attitude toward privacy protection and privacy intention.

[H2] There is a positive relationship between privacy self-efficacy and privacy intention.

[H3] There is a positive relationship between privacy self-efficacy and privacy protection behavior.

[H4] There is a positive relationship between privacy intention and privacy protection behavior.

In addition, this study also explores in whether information ethics education plays a role influencing students' concept in protecting information privacy. Therefore, this study further examines if students attitude toward privacy protection, privacy self-efficacy, privacy intentions, and behavior can be raised through information ethics education. Four extended hypotheses are proposed:

[H5] The semester-long information ethics education does play a role in strengthening the relationship between attitude toward privacy protection and privacy intention

[H6] The semester-long information ethics education does play a role in strengthening the relationship between privacy self-efficacy and privacy intention.

[H7] The semester-long information ethics education does play a role in strengthening the relationship between privacy self-efficacy and behavior.

[H8] The semester-long information ethics education does play a role in strengthening the relationship between privacy intention and behavior.

Methodology

A scenario-based field survey is adopted for conducting the present study because vignettes provide a less-intimidating way to respond to sensitive issues (Harrington, 1996). The scenario used in this study that described the possible invasion of information privacy within a business environment was adapted from Hsu and Kuo (2003) and Kallman (1996), which measured information systems employees' attitudes and intentions. Three constructs, which used multiple-item scales, were measured in this study. The constructs "attitude toward privacy protection" and "privacy intention" were referenced from Ajzen (2002) and Chang (1998). The measurement items used to construct privacy self-efficacy were referenced from Kuo et al. (2007). The three construct items used a seven-point Likert scale anchored between "strongly disagree (=1)" and "strongly agree (=7)". Behavior was measured by a one-item question asking the students to make a choice among possible actions.

Questionnaires were administered to senior-level undergraduate students who had taken a mandatory course of information ethics at the department of Information Management in Taiwan. A total of 140 students agreed to participate voluntarily in the study. The 116 completed surveys constitute an 82.86% response rate. Besides, to response to the second research question for understanding the differences between pre-education and post-education students in the relationships that the effects of attitude toward privacy protection, privacy self-efficacy, and privacy intention have on behavior, the student subjects are asked to answer the first research questionnaire at the term begins the information ethics course. Afterwards, the experimenter (teacher) lecture on information ethics which covered a wide range of information ethics topics, including basic ethical principles, information ethics issues (information privacy, information property right and so on), etc. Students are requested to take different kinds of assignments regarding information privacy issues, such as open questions, brainstorm, and peer discussions during the whole semester. Finally, all students are asked to fill out the second time research questionnaire at the end of the semester. In total, two cross-section data collect in this study, one is delivered at the beginning of the semester, and the second version is delivered at the end of the semester.

Data analysis

All students share the same demographics; their ages range from eighteen to twenty-five years old, and they are senior-level undergraduate students in college and will be graduated in the coming semester.

Reliability and Validity

Cronbach's α and factor analysis are calculated to assess the internal reliability and validity of the scales developed for the study. Table 1 shows the scales generally prove appropriate reliability and validity respectively.

Construct Items	Construct Label			Cronbach's α	
	ATT	PSE	INT	Before education	After education
ATT-1	0.875			0.713	0.706
ATT-2	0.837				
PSE-A		0.809		0.791	0.909
PSE-B		0.786			
PSE-C		0.767			
INT-1			0.933	0.317*	0.456*
INT-2			0.558		
Eigenvalues	1.875	1.799	1.154		
% of Variance	26.783	25.696	16.487		
Cumulative %	26.783	52.479	68.966		

Extraction Method: Principal Component Analysis.
ATT: Attitude toward Privacy Protection; PSE: Privacy Self-Efficacy;
INT: Privacy Intention
* the low alpha is a result of the scale not having enough variability

Table 1: Reliability Cronbach's α and Factor Analysis

Hypothesis testing

An ANOVA analysis of the four research variables shows that significant differences exist between the before and after information ethics education for the following variables: attitude toward privacy protection, privacy self-efficacy, and privacy intention; yet there is no difference in the privacy protection behavior (See Table 2).

Research Construct	Mean		Sig.
Attitude toward privacy protection	Before Education	3.61	0.078*
	After Education	3.94	
Privacy Self-Efficacy	Before Education	4.49	0.053*
	After Education	4.74	
Privacy Intention	Before Education	5.09	0.018**
	After Education	4.67	
Behavior	Before Education	2.17	0.776
	After Education	2.15	
*p < 0.1; **p < 0.05			

Table 2: ANOVA Test for the significance between before and after education

In this research, we have assessed our first four hypotheses using structural equation modeling (SEM) because of its ability to validate casual relationships. We have chosen Smart PLS 2.0.M3 for this analysis. As recommended by Chin (1998), bootstrapping with 500 sub-samples was performed to test the statistical significance of each path coefficient using the t-test. The structural model results of path coefficient and t-value is shown in table 3. These results indicate that hypotheses H1, H2 and H4 are supported, while the H3 is partially supported in the model of after education.

Hypotheses	Before Education		After Education	
	β	t-value	β	t-value
[H1] ATT→INT	0.368	4.489***	0.440	4.494***
[H2] PSE→INT	0.242	2.838***	0.107	1.364*
[H3] PSE→BEH	0.306	1.156	0.293	3.587***
[H4] INT→BEH	0.112	3.199***	0.389	4.939***
ATT: Attitude toward Privacy Protection; PSE: Privacy Self-Efficacy; INT: Privacy Intention; BEH: Privacy Protection Behavior *** p < 0.01; ** p < 0.05; * p < 0.1				

Table 3. Structural model results

Observing the R^2 of the research model, while before information ethics education, the model explains 22% of the variation of privacy intention, and 12.7% of the variation of behavior (shown in Figure 2); after the information ethics education, the

model explains 20.8% of the variation of privacy intention, and 26.5% of the variation of behavior (shown in Figure 3). The R^2 change of behavior from 12.7% to 26.5% shows that the information ethics education plays a role, that is, the construct of privacy self-efficacy and privacy intention have more explanation power in predicting students' behavior concerning information privacy protection.

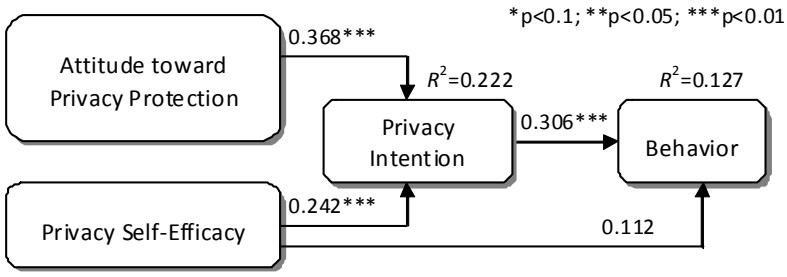

Figure 2: Result of Model test – Before Education

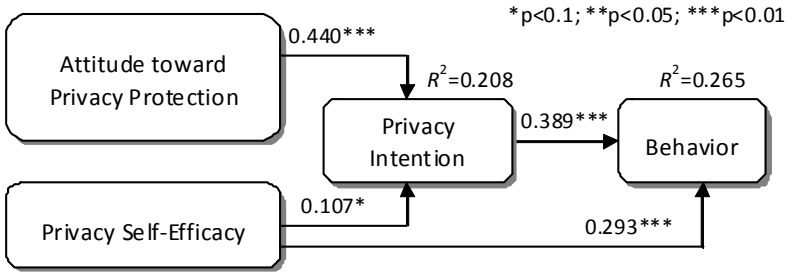

Figure 3: Result of Model test – After Education

A path comparative analysis is employed to test the validity of the last four hypotheses (H5 to H8) in this study (see table 4). The statistical effect can be tested by using the following equation (Chin 2004). The statistical comparison t-test shows that H5 is marginal supported ($t = 1.127$, $p < 0.15$), which reveals that the concept of privacy self-efficacy have more influence on privacy intention before education. H7 is significantly supported ($t = -1.421$, $p < 0.1$), which indicates that the concept of privacy self-efficacy have more impact on behavior after education. The findings exhibit an important insight that through information ethics education, students demonstrate a significant change in their confidence of privacy self-efficacy; the increase of this concept noteworthy changes their behavior concerning information privacy protection.

Hypotheses	Standard errors		Sp	$\beta_{pre} - \beta_{post}$	t-value	result
	Pre	Post				
[H5] ATT→INT	0.085	0.098	1.080	-0.071	-0.514	n.s.
[H6] PSE→INT	0.087	0.078	0.932	0.135	1.127^{+}	Pre > Post
[H7] PSE→BEH	0.096	0.082	0.991	-0.181	-1.421^{*}	Pre < Post
[H8] INT→BEH	0.099	0.081	0.993	-0.083	-0.652	n.s.
ATT: Attitude toward Privacy Protection; PSE: Privacy Self-Efficacy; INT: Privacy Intention; BEH: Privacy Protection Behavior * $p < 0.1$; $^{+}$ $p < 1.5$						

Table 4. The Difference before and after Information Ethics education

CONCLUSIONS

Findings of this study generally support the results of previous studies on self-efficacy theory. Specifically, results from the study shed light on interesting or subtle differences in information ethics education. First, the students' attitude toward privacy protection, privacy self-efficacy, and privacy intention are significantly changed before and after lecturing information ethics course, this supports the importance of the information ethics education. Therefore, we suggest that this course should be a mandatory subject in the IS curriculum. Second, a high percentage of college students in the information management department in Taiwan will work for the IT industry after they graduate. The increased privacy self-efficacy has greatly contributed to develop their fundamental ethical values, which will influence their behavior when faced ethical dilemmas. Furthermore, we might expect that these students who were equipped with information ethics education would behave ethically and avoid unethical behavior.

Today, increasing students' consciousness of IS knowledge and ethics are important strategies for them to deal with quandary in the business environment. Education is a fundamental way to encourage students to act ethically regarding privacy. Particularly most privacy invasions are not dramatic or visible; they creep up on us slowly. Students need to train up their sensibility in recognition the hazard of our privacy being invaded or the violation of others' privacy rights.

APPENDIX

A system analyst, Peter, describes himself as a facilitator and troubleshooter. His primary responsibility is to help all the employees in his company accomplish all the tasks they need to perform on the corporation's local area network. Now, a new utility program called LANSCAPE allows Peter to solve user problems without ever having to go directly to the users' workstation because his screen shows exactly what the user sees. Upon receiving troubled users' calls, his primary task is to run LANSCAPE at his desk and solve their problems. Sometimes Peter proactively scans a number of users without their knowledge, and when he finds one in trouble, he can interrupt and help. Whenever Peter has users' screens showing on his terminal, he will tell them they are being monitored.

One day, Perter's manager says, "through such computer-based monitoring, I can evaluate employees' performance at my desk. I would not reveal this outside the Human Resources Department, but I think I wan to enlist your support." As he doesn't know whether monitoring in this situation is permitted, he frowns and tells his manager, "I don't know if I should give you that software. Let me think about it and get back to you." (Adapted from Hsu and Kuo (2003), original by Kallman and Grillo, 1996)

REFERENCES

1. Ajzen, I. (2002) Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior, *Journal of Applied Social Psychology*, 32, 665-683.
2. Ajzen, I., and Fishbein, M. (1980) Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Englewood Cliffs, NJ.
3. Bandura, A. (1977) Self-efficacy: Toward a Unifying Theory of Behavioral Change, *Psychological Review*, 84, 1, February, 191-215.
4. Bandura, A. (1986) Social Foundations of Thought and Action, Prentice Hall, Englewood Cliffs, NJ.
5. Bandura, A. (1991) Social Cognitive Theory of Moral Thought and Action, in W. M. Kurtines & J. L. Gewirtz (Eds.), *Handbook of Moral Behavior and Development 1*, (Hillsdale, NJ: Erlbaum), 45-103.
6. Bandura, A. (1997) Self-efficacy: The Exercise of Control, New York: Freeman.
7. Chang, M.K. (1998). Predicting unethical behavior: a comparison of the theory of reasoned action on the Theory of Planned Behavior. Journal of Business Ethics, 17, 16, 1828-1834.
8. Chin, W.W. (1998) The Partial Least Squares Approach to Structural Equation Modeling," in Marcoulides, G. A. (eds.), *Modern Methods for Business Research*, NJ Lawrence Erlbaum Associates.
9. Chin, W.W. (2004) Frequently Asked Questions – Multi-Group Analysis with PLS (updated December 21, 2004), available at http://disc-nt.cba.uh.edu/chin/plsfaq/multigroup.htm.

10. Clarke, R.A. (1988) Information Technology and Dataveillance, *Communications of the ACM*, 31, 5, 498-512.
11. Compeau, D.R. and Higgins, C.A. (1995) Computer Self-Efficacy: Development of a Measure and Initial Test, *MIS Quarterly*, 19, 2, 189-211.
12. Gentile, M. and Sviokla, J.J. (1990) Information Technology in Organizations: Emerging Issues in Ethics & Policy, note, Harvard Business School, Boston, MA.
13. Gist, M.E. and Mitchell, T. R. (1992) Self-Efficacy: A Theoretical Analysis of Its Determinants and Malleability, *Academy of Management Review*, 17, 2, 183-211.
14. Harrington, S.J. (1996) The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions, *MIS Quarterly*, September, 257-278.
15. Henry, J. W., and Stone, R. W. (1999) The Impacts of End-User Gender, Education, Performance, and System Use on Computer Self-Efficacy and Outcome Expectancy, *Southern Business Review*, 10-16.
16. Hill, T., Smith, N.D., and Mann, M.F. (1987) Role of Efficacy Expectations in Predicting the Decision to Use Advanced technologies: The Case of Computers, *Journal of Applied Psychology*, 72, 2, 307-313.
17. Hsu, M.H and Kuo, F.Y. (2003) The Effect of Organization-Based Self-Esteem and Deindividuation on Protecting Personal Information Privacy. *Journal of Business Ethics*, 42, 4, February, 305-320.
18. Kallman, E.A. and Grillo J.P. (1996) Ethical Decision Making and Information Technology: An Introduction with Cases, Second Edition. New York: McGraw-Hill.
19. Kuo, F., Lin, C.S., Hsu, M. (2007) Assessing gender differences in computer professionals' self-regulatory efficacy concerning information privacy practices. *Journal of Business Ethics*, 73, 145-160.
20. Latham, G.P. and Frayne, C.A. (1989) Self-management Training for Increasing Job Attendance: A Follow-up and a Replication, *Journal of Applied Psychology*, 74, 411-416.
21. Marakas G.M., Yi M.Y., and Johnson R.D. (1998) The Multilevel and Multifaceted Character of Computer Self-Efficacy: Toward Clarification of the Construct and an Integrative Framework for Research, *Information Systems Research*, 9, 2, June, 126-163.
22. Mason, R. O. (1986) Four Ethical Issues of the Information Age, *MIS Quarterly*, 10, 1, March, 5-12.
23. Miller, A. (1971) The Assault on Privacy: Computers, Data Banks and Dossiers, University of Michigan Press, Ann Arbor, MI.
24. Westin, A.F. (1967) Privacy and Freedom, Atheneum Publishers, New York.