Creative Education, 2016, 7, 171-179
Published Online January 2016 in SciRes. http://www.scirp.org/journal/ce
http://dx.doi.org/10.4236/ce.2016.71017

Educating Students' Privacy Decision Making through Information Ethics Curriculum

Cathy S. Lin

Department of Information Management, National University of Kaohsiung, Taiwan
Email: cathy@nuk.edu.tw

Received 6 October 2015; accepted 26 January 2016; published 29 January 2016

Abstract

Increasingly sophisticated technologies nowadays have equipped powerful capabilities to obtain and exploit consumers' information privacy on the Internet. The contemporary privacy protection techniques seem fail to guard information privacy. Besides of the technological protections, information ethics education is described as the ideal way to increase people's consciousness. This study proposes a privacy decision making model which posits that attitudes toward privacy protection, privacy self-efficacy for protection, and privacy self-efficacy for non-acquisition are critical factors essential to behavioral intention. Further, a longitudinal model explores whether information ethics education plays a role in influencing students' concepts of protecting information privacy. A survey of 111 senior-level undergraduate students in the department of Information Management was conducted to test the hypothesized model. The findings exhibit important insights: through information ethics education, students demonstrate significant model paths changes in the relationships of attitude, privacy self-efficacy for protection, and privacy self-efficacy for non-acquisition to intention. The implications to the ethics curriculum concerning information privacy are discussed.

Keywords

Privacy, Self-Efficacy, Decision Making, Information Ethics, Ethics Curriculum

1. Introduction

The rapidly technological developments have enhanced our life, which brings much convenience and efficiency to data collection, and data processing to generate data value proliferation. While these computing technologies

How to cite this paper: Lin, C. S. (2016). Educating Students' Privacy Decision Making through Information Ethics Curriculum. *Creative Education, 7,* 171-179. http://dx.doi.org/10.4236/ce.2016.71017

become more powerful and sophisticated, the issue of privacy has surfaced to become one of the most critical concerns. For example, the confidentiality and anonymity are battered by using data analytics algorithm, individuals preferences can be easily derived from various online sources (i.e. personal website, blogs, social networking sites, etc.). A recent study by Kosinski, Stillwell, & Graepel (2013) show that Facebook "Likes" can be used to automatically predict sensitive personal attributes, such as religious and political views, even family connections. The privacy loss in the information age is significant, confirmed by the United States' President's Council of Advisors on Science and Technology (PCAST) report[1] about "Big Data and Privacy": "big data analytics have the potential to eclipse long-standing civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace" (House, 2014).

Nowadays, the public have perceived a ubiquitous threat from information technologies, which are equipped with enhanced capabilities for surveillance, storage, retrieval, and transmission of personal information (Clarke, 1988; Mason, 1986). Looking back the contemporary privacy protection technologies, the existing protection methods and techniques seem fail to achieve this goal in guarding information privacy. In addition to technological protections, we are calling for an essential way to raise people's consciousness of information privacy. Moreover, while this study conducts in Taiwan, the term "privacy" under Chinese culture is a fragile and vague perception, which traditionally is treated as a right that authority owns; those disadvantaged minorities often have to sacrifice their privacy to gratify the authority's interest. Under such circumstances, arousing the consciousness of privacy is valuable and needed. According to a recent study by Lin & Chou (2014) that investigated ethics-related courses related to information ethics in Taiwan 118 universities during 2010 to 2012, the results showed that the information ethics curricula has not yet prevalent offered in the universities, therefore calling for the necessity of higher education on information ethics.

This study aims at cultivating one's privacy decision making through a semester information ethics education. The theory of self-efficacy is adopted from the social-psychological perspective, the main construct of privacy self-efficacy is examined to see the vignette decisions related to information privacy change before and after lectures. In the proposed model, this study tries to demonstrate whether information ethics education can significantly influence students' attitudes toward privacy protection, two kinds of privacy self-efficacy (protection and non-acquisition), and privacy intention. The values of this study will be helpful for understanding individuals privacy self-efficacies, and schools/educators should consider cultivating consciousness of information privacy issues in IS professional ethical curriculum. Two research issues are listed:

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

RQ2: Significant differences have been recognized between pre-education and post-education IS students in the relationships that the attitudes, and privacy self-efficacy have impacted on behavioral intention.

2. Literature Reviews

2.1. The Necessity of Information Ethics Education

Technological advances in the information age have led many people to believe that the coverage of ethics in universities is the best way for students to form their perceptions of ethics, and preparing students to deal with ethical issues in information society. Ethics training or ethics education concerning information systems are not a "one time" inoculation. No matter the school education and on the job training concerning information ethics issues have been proven to increase the probability, individuals will practice more ethical behaviors on the job. For example to the ethical education, Smith, Fryer-Edwards, Diekema, & Braddock (2004) claimed that ethical education arouse students' recognition of common ethical dilemmas. Almagno & Carbo (2001) introduced a series information ethics courses to bachelor, master, and doctoral level students. After taking the course, the graduates report that the courses have had a much greater effect on their personal and professional lives than other courses. As for the example about ethical training in practices, codes of ethics have been found to effectively deter unethical behaviors and provide more specific guidance to computing professionals (Oz, 1992); the work by Harrington (1996) has also demonstrated that ethical rules written specifically to deal with software issues have positive effect on computer abuse judgments and intention.

In the computer science domain, several main professional institutions have drawn up explicit codes of ethics

[1] http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

and computer professional responsibilities into schools and association curricula. For example, the 1992 Computer Sciences Accreditation Board (CSAB), the 1992 Association for Computing Machinery Computing Curricula (ACM), the 2006 Association of Information Technology Professionals (AITP), and 2006 Institute of Electrical and Electronics Engineers Software Engineering Code of Ethics (IEEE-CS). The reason these professional associations draw up explicit codes and incorporate ethical issues as a part of the standard curriculum is to educate students and IT workers knowing information systems professional responsibility about ethics issues, further helping handling conflicts when facing ethical dilemmas. Just as the ethical curriculum of CSAB requirements, four clearly goals are listing: 1) to aid students in becoming computer professionals; 2) to help students accept the responsibilities associated with being an IT professional; 3) to encourage students to formulate and express their views on social and legal issues; and 4) to raise students' awareness of the impact computing has on society. However, a recent study by Lin & Chou (2014) investigated information ethics-related courses in Taiwan and showed that the information ethics curricula has not yet prevalent offered in the universities, it is of necessity calling for higher education on information ethics.

2.2. Self-Efficacy Theory

Self-efficacy refers to one's belief that he or she has the capability to execute a particular action, which is a major determinant of what activities people will choose, how much effort they will expend, and how long they will sustain the effort in dealing with stressful situations (Bandura, 1997). The concept of self-efficacy has been widely studied and proven to be a critical predictor of human conduct in various settings, such as learning, health-promoting behavior, clinical functioning, athletic achievement, and career and occupational development. It is an important element of Social Cognitive Theory (SCT), which adopts a cognitive interactionist perspective to personal behavior. In this framework, people's efficacy beliefs play an important role in mediating their goal setting, thought patterns, emotional states, and strategies and actions chosen.

In the ethics domain, Bandura (1991) has elaborated the "Social Cognitive Theory of Moral Thought and Action" and has presented the view that an explanation of the relation between ethical reasoning and conduct must specify the psychological mechanisms by which moral standards get translated into actions. SCT asserts that moral conduct is motivated and regulated mainly by the ongoing exercise of self-regulatory efficacy. Effective self-regulation of conduct requires not only obvious self-regulatory skills but also a strong belief in one's own capabilities to achieve personal control. Therefore, people's beliefs in their efficacy to exercise control over their own motivations, thought patterns, and actions play important roles in the exercise of human agency (Bandura, 1986). The stronger the perceived self-regulatory efficacy, the more persevering are people in their self-controlling efforts, and the greater is their success in resisting social pressures to behave in ways that violate their standards; on the contrast, a low sense of self-regulatory efficacy heightens vulnerability to social pressures for transgressive conduct (Bandura, 1991: p. 69).

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; Marakas, Yi, & Johnson, 1998). Several empirical studies found that self-efficacy would play an even greater role if IS professionals were required to be aggressive in challenging organizational information privacy policies (Korzaan, Brooks, & Greer, 2009; Smith, 1993; Smith, Milberg, & Burke, 1996). Moreover, researchers in IS-related studies have explored how the expectation of computer self-efficacy may impact decisions concerning technology acceptance and usage (Compeau & Higgins, 1995; Gist & Mitchell, 1992; Henry & Stone, 1999). For the reasons given above, this research relies on Bandura's self-efficacy theory to address whether strengthening perceived self-efficacy will increase IS students' capability concerning protecting information privacy.

2.3. Research Model

Previous theories such as theory of reasoned action (TRA) and theory of planned behavior (TPB) have theorized that attitudes and intentions are the best predictors of specific behaviors (Ajzen, 1991, 2002; Ajzen & Fishbein, 1980). In this study, perceived self-efficacy is included as an attempt to strengthen the individual's behavioral intentions, the importance of self-efficacy as a predictor of behavior is greater in activities in which the person has only variable or limited control over behavior (Ajzen, 2002). Based on the work by Kuo, Lin, & Hsu (2007), two kinds of privacy self-efficacy are covered to simultaneously see the impact on individual's privacy intention. Therefore, this research posits a privacy decision making model that attitude toward privacy protection, privacy self-efficacy for protection, and privacy self-efficacy for non-acquisition are critical factors essential to behavioral intention (see **Figure 1**).

In this model, three basic hypotheses are examined:

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

[H2] There is a significant relationship between privacy self-efficacy for protection and privacy intention.

[H3] There is a significant relationship between privacy self-efficacy for non-acquisition and privacy intention.

In addition, this study aims at exploring the role of information ethics education in influencing students' concepts concerning information privacy. Therefore, a semester longitudinal model is compared: Time 1 represents the period before students have had formal education in information ethics, and Time 2 (a semester later) represents the period after students have mastered the information ethics course. This design is intended to see whether the model paths for Time 1 (before information ethics education) significant difference from those paths for Time 2 (after education). Therefore, three extended hypotheses are proposed:

[H4] There is a significant path difference between pre-education and post-education students in the relation between attitude toward privacy protection and privacy intention.

[H5] There is a significant path difference between pre-education and post-education students in the relation between privacy self-efficacy for protection and privacy intention.

[H6] There is a significant path difference between pre-education and post-education students in the relation between privacy self-efficacy for non-acquisition and privacy intention.

3. Methodology

3.1. Research Procedure

Every student was asked to fill out the questionnaire at the beginning of the information ethics course (Time 1). During the information ethics course, the course design are described in the following: First, the teacher lectured fundamental knowledge concerning a wide range of information ethics topics, including basic ethical principles and information ethics issues (information privacy, information property rights, freedom of speech, and so on). Second, teaching strategies cover problem-based instruction to raise students' moral imagination, and case-based instruction to have students open discussions on ethical dilemmas. Finally, the values clarification strategy is used to conclude by teacher.

Through information ethics education, students are situated in the vignettes concerning information privacy (and other information ethics topics). Vignettes feature ethical dilemmas among competing ethical principles that can be addressed, which are meant to be a kind of teaching tools, more specific, the vignettes create a problem-solving approach to call for students taking part in how to make ethical decision making. After the vignettes discussions, students have to document the decision-making process as the case assignments. At the end of the semester, all students were asked to fill out the second questionnaire at the end of the semester (Time 2).

3.2. Vignette Design

A scenario-based field survey was adopted for conducting the present study. Due to the sensitive nature of ethical conduct, vignettes have the advantages of providing a quasi-way to respond to sensitive issues and offering

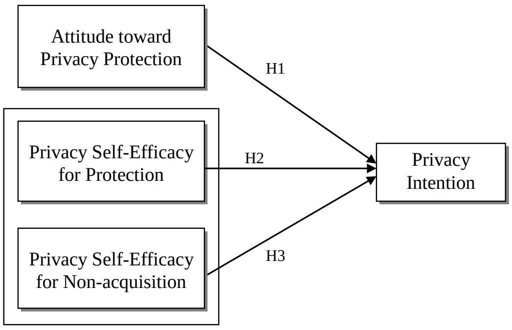
Attitude toward Privacy Protection
Privacy Self-Efficacy for Protection
Privacy Self-Efficacy for Non-acquisition
H1
H2
H3
Privacy Intention

Figure 1. Research model.

realistic scenarios that place the subject in a decision-making role. Such vignettes are commonly used in ethics research (Banerjee, Cronan, & Jones, 1998; Harrington, 1996).

In this study, to reflect the research issue concerning information privacy, the design of the scenario used in this study adapts privacy case IV.1 from the American Federation of Information Processing Societies (AFIPS) scenario collection (Parker, Swope, & Baker, 1990), the case describes a the scenario concerning revealing a system's inadequate protection of privacy. The subjects were placed in decision-making roles for the targeted privacy protection behavior; that is, whether to fix the back-door deficiency of the computing system even though customers may not aware the possible invasion of personal information.

3.3. Constructs and Operationalization

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). The construct of "attitude toward privacy protection" refers to the individual's feeling for the behavior to fix the back-door deficiency of the computing system, which consists of two items, an example item from this scale was "The decision is beneficial to the companies." The construct of "privacy intention" refers to the individual's decision to fix the back-door deficiency of the computing system, which consists of two items, an example item from this scale was "If I were the IS employee in this story, I would plan to behave the same as he did." The measurement items used to construct privacy self-efficacy were referenced from Kuo et al. (2007). The construct of "privacy self-efficacy for protection" refers to whether an individual can take the necessary courses of action for guarding accidental disclosures of information in a public environment, which consists of two items, an example item from this scale is: "If you happen to find that some customers' privacy information is revealed on the network, how confident are you to protect this information immediately?" As for the construct of "privacy self-efficacy for non-acquisition" refers to whether a person has the self-confidence to refuse to acquire and use privacy information before he or she obtains the necessary authorization or permission to do so, which consists of six items, an example item is: "If you have the means to access the privacy information concerning your customers beyond the delegated situation, how confident are you not to take advantage of this situation?" All the research construct items used a seven-point Likert scale anchored between "strongly disagree (=1)" and "strongly agree (=7)".

3.4. Participants

As the amount of businesses and individuals information continue to grow and the access to that information by IT personnel increases, ethics cognition and value judgments by IT professionals becomes more important. Especially for those students who major in information systems, an obligation to understand the responsibility that goes with their IS profession is imperative. Their values concerning information privacy will affect how they write programs, manage privacy and security issues, and handle critical software and computing.

Therefore, the students who majored in the department of information management are chosen as the participants in this study. All participating students were senior-level undergraduate students from the universities in the south of Taiwan. In-class paper-and-pencil survey was administered to the subjects at their information ethics course. A total of 150 students from three classes voluntarily agreed to participate in the study. The 111 subjects completed both Time 1 and Time 2 surveys constitute a 74% valid dataset. The subjects were at this time taking the information ethics course; therefore, they shared the same demographics that ages ranged from 18 to 25 years, 58% are male students and 42% are female students.

4. Data Analysis

4.1. Reliability and Validity

Exploratory factor analyses were used to assess convergent and discriminant validity. The results showed that values for the factor loadings were between 0.587 - 0.931. All factor loadings were greater than 0.5 and all were statistically significant at $p < 0.01$, suggesting that the measures satisfied convergent validity. All eigenvalues associated with the factors exceeded the required level of 1.0, varying from 1.14 to 3.73. Principal components analysis was used as the extraction method for factor analysis with Varimax rotation. As shown in **Table 1**, the overall factor structural solution had an appropriate loading pattern and explained 68.94 percent of the variation.

An analysis of variance (ANOVA) of the four research variables shows that significant differences exist

Table 1. EFA loading structures for antecedent research constructs.

Constructs	Item	Factor loading				Rotation sums of squared loadings	
		1	2	3	4	Eigenvalues	Cumulative %
Attitude toward privacy protection	AT1	**0.931**	0.157	0.033	0.352	3.73	31.08%
	AT2	**0.820**	0.103	0.059	0.225		
Privacy self-efficacy for protection	PP1	0.139	**0.905**	0.307	0.085	1.76	45.73%
	PP2	0.138	**0.902**	0.335	0.083		
Privacy self-efficacy for non-acquisition	PA1	0.121	0.322	**0.769**	0.121	1.65	59.46%
	PA2	0.048	0.341	**0.587**	0.030		
	PA3	0.055	0.241	**0.642**	0.018		
	PA4	0.021	0.313	**0.864**	0.150		
	PA5	0.083	0.299	**0.802**	0.092		
	PA6	0.036	0.273	**0.865**	0.135		
Privacy intention	INT1	0.182	0.040	0.090	**0.587**	1.14	68.94%
	INT2	0.311	0.090	0.143	**0.881**		

between the "before" and "after" information ethics education groups for the following variables: attitude toward privacy protection, and privacy self-efficacy for non-acquisition, yet there is no difference in privacy self-efficacy for protection and intention. More specific, through a semester long course teaching, students raise their concept about attitude toward privacy protection and privacy self-efficacy for non-acquisition (see **Table 2**).

Table 3 shows the values of composite reliability (CR), and average variance extracted (AVE). The reliability CRs exceeded the level of 0.50 recommended by Fornell (1982); their values varied from 0.560 to 0.816, confirming the internal consistency of the constructs' items. The AVE estimates, ranged from 0.710 to 0.899, exceeded the 0.50 lower limit recommended by (Fornell & Larcker, 1981), supporting convergent validity. In addition, the correlation between each pair of research constructs were less than the AVE estimate of each construct (Segars & Grover, 1998), therefore supporting discriminant validity.

4.2. Hypothesis Testing

In this research, we have assessed our first four hypotheses by using the structural equation modeling (SEM) due to its ability to validate causal relationships. We have chosen Smart PLS 2.0.M3 for this analysis (Ringle, Wende, & Will, 2005). As recommended by Chin (1998), bootstrapping with 500 subsamples 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 are shown in **Table 4**. These results indicate that hypotheses H1 and H3 are supported, whereas hypothesis H2 is partially supported in the model of post-education.

The path coefficients show some interesting findings. The relationship between attitude and intention (H1: from 0.213 to 0.461), between privacy self-efficacy for protection and intention (H2: from 0.104 to 0.151), and between privacy self-efficacy for non-acquisition and intention (H3: from 0.222 to 0.278) have significant increases, which demonstrates the value of information ethics education. Regarding the R^2 of the research model, before information ethics education, the model explains 10.1% of the variation of privacy intention; after information ethics education, the model explains 27.3% of the variation of privacy intention. The significant R^2 change of privacy intention shows that a semester long information ethics education plays a role.

A path comparative analysis is employed to test the last three hypotheses, the statistical effect can be tested by using the formula provided by Sarstedt, Henseler, & Ringle (2011). A statistical comparison t-test shows that hypothesis H4, H5, and H6 are supported, as shown in **Table 5**. The findings exhibit an important insight: through information ethics education, students demonstrate significant model paths changes in the relationships of attitude, privacy self-efficacy for protection, and privacy self-efficacy for non-acquisition to intention.

Table 2. ANOVA test for the significance between groups before and after education.

Research Construct	Mean (Std)		Sig.
Attitude toward privacy protection	Before Education	3.635 (1.527)	0.08^{*}
	After Education	3.955 (1.250)	
Privacy self-efficacy for protection	Before Education	3.566 (1.266)	0.55
	After Education	3.466 (1.247)	
Privacy self-efficacy for non-acquisition	Before Education	4.280 (1.094)	0.05^{**}
	After Education	4.568 (1.095)	
Privacy intention	Before Education	3.929 (1.041)	0.78
	After Education	3.891 (0.989)	

$^{*}p < 0.1$; $^{**}p < 0.05$.

Table 3. Reliability and validity among constructs.

Constructs	Mean (Std)	CR	AVE	1	2	3	4
1. Attitude toward privacy protection	3.795 (1.401)	0.769	0.869	1			
2. Privacy self-efficacy for protection	3.516 (1.255)	0.816	0.899	0.153	1		
3. Privacy self-efficacy for non-acquisition	4.424 (1.102)	0.581	0.891	0.049	0.355	1	
4. Privacy intention	3.910 (1.013)	0.560	0.710	0.341	0.093	0.160	1

Table 4. Structural model results.

Hypotheses	Before education		After education	
	β	t-value	β	t-value
[H1] Attitude → intention	0.213	2.354^{**}	0.461	5.684^{***}
[H2] PSE for protection → intention	0.104	1.283	0.151	1.879^{*}
[H3] PSE for non-acquisition → intention	0.222	2.619^{**}	0.278	2.884^{**}
R^2 for dependent variable of intention	10.1%		27.3%	

$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

Table 5. Differences before and after information ethics education.

Hypotheses	Standard errors		$\lvert B_{pre} - \beta_{post}\rvert$	t-value
	Pre	Post		
[H4] Attitude → intention	0.213	0.461	0.247	19.707^{***}
[H5] PSE for protection → intention	0.104	0.151	0.047	3.220^{**}
[H6] PSE for non-acquisition → intention	0.222	0.278	0.056	1.967^{**}

$^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

5. Conclusion

From the findings of this study, the hypotheses are supported and confirmed that the necessity of information ethics education helps nurturing students' privacy decision making. Specifically, results from the study shed light on interesting or subtle differences in information ethics education. It is a semester long information ethics course that helps IS students strengthening the relationships between attitudes, two kinds of privacy self-efficacy and privacy intention. This study specific explores two kinds of privacy self-efficacy for both "protection" and "non-acquisition" which will influence one's behavior when individual faces with information privacy dilemmas in the workplace. Findings of this study generally support the results of previous studies on self-efficacy theory.

Corresponding the findings of this study with the four goals of CSAB requirements, this study demonstrates that information ethics course helps students to be situated in the vignettes concerning information privacy (and other information ethics topics), as a result, this study confirms that the benefits of information ethics education are to encourage students to articulate and express their views on social and legal issues concerning information society; also, the scenario-based case discussion places students in the situation concerning the impact of computing on the information society to help raising their introspection. Especially for those students who major in information systems, an obligation to understand the responsibility that goes with their IS profession is imperative. Therefore, the information ethics course also aids students in becoming qualify information systems professionals; and helps students accepting the responsibilities associated with being information systems professionals. In the long run, it is expected that those students who were equipped with information ethics literacy would behave more ethically and choose not to act unethically.

Nowadays, most information privacy invasions are not dramatic or visible; they creep up slowly, especially true for the online environment. Students need to sharpen their sensibilities in recognizing the hazards of invasion of privacy or violation of privacy rights of others. The findings of this study strongly recommend that the information ethics course can be the professional ethics training in school, which should be a mandatory subject in IS curriculum. Especially a high percentage of college students in the department of information management will work as the information workers after they graduate. Therefore, increasing students' consciousness of IS knowledge and ethics constitutes an important strategy to coach students in dealing with quandaries in the business environment.

Acknowledgements

This paper was supported by the National Science Council of Taiwan under Grant NSC101-2410-H-390-004-MY3. The author wishes to acknowledge the comments offered by the anonymous reviewers.

References

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50,* 179-211. http://dx.doi.org/10.1016/0749-5978(91)90020-T

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.

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Almagno, S., & Carbo, T. (2001). Information Ethics: The Duty, Privilege and Challenge of Educating Information Professionals. *Library Trends, 49,* 510-518.

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice-Hall, Inc.

Bandura, A. (1991). Social Cognitive Theory of Moral Thought and Action. In W. M. Kuritines, & J. L. Gewirtz (Eds.), *Handbook of Moral Behavior and Development* (Vol. 1, pp. 45-103). Hillsdale, NJ: Lawrence Erlbaum Associates.

Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: W.H. Freeman.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics. *MIS Quarterly, 22,* 31-60. http://dx.doi.org/10.2307/249677

Chin, W. W. (1998). The Partial Least Squares Approach for Structural Equation Modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM, 31,* 498-512. http://dx.doi.org/10.1145/42411.42413

Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly, 19,* 189-211.

Fornell, C. (1982). *A Second Generation of Multivariate Analysis: Methods*. New York: Praeger.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18,* 39-50. http://dx.doi.org/10.2307/3151312

Gist, M. E., & Mitchell, T. R. (1992). Self-Efficacy: A Theoretical Analysis of Its Determinants and Malleability. *Academy* *of Management Review, 17*, 183-211.

Harrington, S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly, 20,* 257-278. http://dx.doi.org/10.2307/249656

Henry, J. W., & 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, 25,* 10.

House, W. (2014). Big Data: Seizing Opportunities, Preserving Values. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

Korzaan, M., Brooks, N., & Greer, T. (2009). Demystifying Personality and Privacy: An Empirical Investigation into Antecedents of Concerns for Information Privacy. *Journal of Behavioral Studies in Business, 1,* 1-17.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private Traits and Attributes Are Predictable from Digital Records of Human Behavior. *Proceedings of the National Academy of Sciences, 110,* 5802-5805. http://dx.doi.org/10.1073/pnas.1218772110

Kuo, F. Y., Lin, C. S., & Hsu, M. H. (2007). Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices. *Journal of Business Ethics, 73,* 145-160.

Lin, C. H., & Chou, C. (2014). Ethics Curricula of the Information Science Departments in Taiwanese Universities and Colleges. *Journal of Research in Education Science, 59,* 197-228.

Marakas, G. M., Yi, M. Y., & 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,* 126-163. http://dx.doi.org/10.1287/isre.9.2.126

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10,* 5-12. http://dx.doi.org/10.2307/248873

Oz, E. (1992). Ethical Standards for Information Systems Professionals: A Case for a Unified Code. *MIS Quarterly, 16,* 423-433. http://dx.doi.org/10.2307/249729

Parker, D. B., Swope, S., & Baker, B. N. (1990). *Ethical Conflicts in Information and Computer Science, Technology, and Business*. Wellesley, MA: QED Information Sciences.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0. Hamburg. http://www.smartpls.de

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results. *Advances in International Marketing, 22,* 195-218. http://dx.doi.org/10.1108/S1474-7979(2011)0000022012

Segars, A. H., & Grover, V. (1998). Strategic Information Systems Planning Success: An Investigation of the Construct and Its Measurement. *MIS Quarterly, 22,* 139-163. http://dx.doi.org/10.2307/249393

Smith, H. J. (1993). Privacy Policies and Practices: Inside the Organizational Maze. *Communications of the ACM, 36,* 104-122. http://dx.doi.org/10.1145/163298.163349

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20,* 167-196. http://dx.doi.org/10.2307/249477

Smith, S., Fryer-Edwards, K., Diekema, D. S., & Braddock, C. H. (2004). Finding Effective Strategies for Teaching Ethics: A Comparison Trial of Two Interventions. *Academic Medicine, 79,* 265-271. http://dx.doi.org/10.1097/00001888-200403000-00015