Journal of Business Ethics (2007) 73:145–160
DOI 10.1007/s10551-006-9179-1

Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices

Feng-Yang Kuo
Cathy S. Lin
Meng-Hsiang Hsu

ABSTRACT. Concerns with improper collection and usage of personal information by businesses or governments have been seen as critical to the success of the emerging electronic commerce. In this regard, computer professionals have the oversight responsibility for information privacy because they have the most extensive knowledge of their organization's systems and programs, as well as an intimate understanding of the data. Thus, the competence of these professionals in ensuring sound practice of information privacy is of great importance to both researchers and practitioners. This research addresses the question of whether male computer professionals differ from their female counterparts in their self-regulatory efficacy to protect personal information privacy. A total of 103 male and 65 female subjects surveyed in Taiwan responded to a 10-item questionnaire that includes three measures: *protection* (protecting privacy information), *non-distribution* (not distributing privacy information to others), and *non-acquisition* (not acquiring privacy information). The findings show (1) significant gender differences exist in the subjects' overall self-regulatory efficacy for information privacy, and, in particular, (2) that female subjects in this study exhibited a higher level of self-regulatory efficacy than males for the protection and non-acquisition of personal privacy information. The identification of the factorial structure of the self-regulatory efficacy concerning information privacy may contribute to future research directed to examining the links between privacy efficacy and psychological variables, such as ethical attitude, ethical intention, and self-esteem. Studies can also be extended to investigate how different cultural practices of morality and computer use in men and women may shape the different development patterns of privacy self-efficacy. Understanding the different cultural practices may then shed light on the social sources of privacy competence and the appropriate remedies that can be provided to improve the situation.

KEY WORDS: gender, information privacy, self-regulatory efficacy

Feng-Yang Kuo holds a B.S. degree in Management Science from Chiao-Tung University, Taiwan and a Ph.D. degree in Information Systems from University of Arizona. He was a faculty of Information Systems at University of Colorado at Denver from 1985 to 1997 and is currently an Associate Professor of Information Management in Sun Yat-Sen University, Taiwan. He has published articles in Communications of ACM, MIS Quarterly, Communications of AIS, Journal of Business Ethics, Information & Management, Journal of Systems and Software, Decision Support Systems, *and* Sun Yat-Sen Management Review. *Among his current interests are information ethics, managerial cognition, and human-computer interfaces.*

Cathy S. Lin is an Assistant Professor of Information Management at National University of Kaohsiung, Taiwan. Her Ph.D. is in Management Information Systems from National Sun Yat-Sen University. She has published Articles in the Information & Management, Journal of Information Management, *and* Sun Yat-Sen Management Review. *Among her current interests are information ethics, ethical decision making, electronic commerce, and information management.*

Meng-Hsiang Hsu is a professor of Information Management at National Kaohsiung of First University of Science and Technology. His Ph.D. is in Management Information Systems from National Sun Yat-Sen University. He has published articles in the Journal of Business Ethics, Behavior & Information Technology, Decision Support System, *and* Industrial Management and Data Systems. *Among his current interests are knowledge management, information ethics, strategic information systems, and electronic commerce.*

Introduction

In tandem with the dramatic increase in digital data, privacy concerns related to the disclosure of personal information have emerged globally (Mason, 1986; Smith, 1994). Privacy issues are further exacerbated now that the World Wide Web makes it easy, convenient, inexpensive, and profitable for data to be automatically collected. These concerns have been seen as threats to electronic commerce and the emerging digital economy. Several surveys of electronic commerce have found that many online consumers decline to provide information requested by the web site or provide false information when that site does not post clear privacy policies concerning why and how personal information is collected and used (Georgia Tech Research Corporation, 1997; Privacy and American Business, 1997).

To computer professionals, privacy issues are especially significant because these professionals develop systems that collect, store, analyze, and distribute online consumers' data. The relationship between computer professionals and personal privacy is similar to most other professional relationships in terms of knowledge and reliance. Lay people trust their interests to experts. People approach a physician for help because the physician has knowledge that they do not have. This is the main reason why a profession such as medicine needs an ethical code of conduct. Similarly, computer professionals possess expertise that others do not and, through their work, they develop an intimate understanding of what is to be done with the data and have the most extensive knowledge of their organization's practices concerning information privacy (Oz, 1992). Yet, computer professionals themselves are possible perpetrators of information privacy invasion and unauthentic accessibility (Harrington, 1995). As a result, their obligations to the clients' information privacy resemble those of other professionals, and how they may exercise sound practices of information privacy in their work becomes a fundamental issue in ethical research concerning information use.

Gender differences in ethical situations

In computer-related behaviors, a number of previous studies have shown that gender differences do indeed exist. Many past studies have shown that women act differently from men in ethical situations (Beltramini et al., 1984; Chonko and Hunt, 1985; Ferrell and Skinner, 1988; Jones and Gautschi, 1988; Kidwell et al., 1987; Reiss and Mitra, 1998; Ruegger and King, 1992; Whipple and Swords, 1992). For example, Dawson (1997) asked 209 sales professionals to respond to 20 ethical scenarios, half of which were "relational" and half "nonrelational." The findings concluded that there were significant ethical differences between gender in situations that involve relational issues, but not in nonrelational situations. More recently, Radtke (2000) asked 51 practicing accountants from public accounting and private industry to evaluate 16 ethically sensitive situations. Significant gender differences related to ethics were found for five of the situations. Related to misuse of computers, many studies have found that females in general act differently from males in resolving problems concerning computer/Internet usage (Adam, 2000; Bissett and Shipton, 1999; Escribano et al., 1999). For instance, Kerie and Cronan (1998) explored moral decision-making in relation to a set of computer ethics cases and inferred that men and women were distinctly different in their assessments of unethical behaviors. Loch and Conger (1996) also found that individual differences such as gender, age, and education may affect people's ethical conduct. In addition, Khazanchi (1995) found that women outperformed men in identifying unethical actions. Mason and Mudrack (1996) explored the gender differences in computer ethics from the gender socialization theory and concluded that women appeared more ethical than men (Mason and Mudrack, 1996, p. 599).

Finally, several studies have consistently shown that the interests of males in privacy-related issues differ from those of females. For example, Sheehan (1999) conducted a survey involving online information gathering and privacy and showed that women generally appeared to be more concerned than men about the effect of that practice on their personal privacy. Westin (1997) also pointed out that more women than men were "very concerned" about threats to privacy today and felt that new laws were needed for confidentiality and control of specific types of information, such as medical

records, insurance information, and financial data, in order to protect privacy.

Research purpose

In sum, computer professionals in the information age have encountered situations that are doubtful, equivocal, and commonly laden with value conflict. Many opportunities and temptations exist for the invasion of information privacy. Some past research has shown that men and women differ in their technical computer competence, while other studies have suggested that men and women also differ in their ethical judgment concerning issues such as privacy. Note that in the computer related professions, the lack of representation of women has been of concern to many policy makers. An early study by Truman and Baroudi (1994) has shown that discriminatory practices exist in the computer-related occupations. More recently, Panteli et al. (1999a, 1999b, 2001) have also shown that the IT industry is not gender-neutral, and that it in fact fails to adequately promote or retain its female workforce. Similarly, Robertson et al. (2001) discovered indirect, deep-rooted discrimination to be the major reason for the segregation and declination of the female workforce in the field of computing in Europe during the 1990s.

What may this lack of female representation mean to the ethical climate of the entire computer occupation, considering that computer professionals now hold key positions in taking care of privacy data? This research sets out to answer this question by investigating gender differences in computer professionals' self-regulatory efficacy concerning information privacy practices. Note that for the study of gender ethics, Adam et al. (2004) have cautioned against the ''essentialist approach'' which assumes the existence of fixed, or even biological, male and female characteristics that determine the behavioral differences in gender. We concur and choose to rely on the theory of self-efficacy, which emphasizes the triadic, reciprocal influences of personal, behavioral, and environmental factors in the development of one's competence in dealing with ethical dilemmas (Bandura, 1991a). In this theoretical formulation, privacy self-efficacy can be considered as a variable that reflects cultural influences on personal self-regulatory beliefs rather than a fixed characteristic of gender. In the next section, we review the theoretical basis that we adopt for our study. Specifically, to probe the concept of self-regulatory efficacy, our investigation relies on Bandura's work in the theory of social cognition and self-efficacy (Bandura, 1986). This section is followed by a presentation of the dimensions of self-regulatory efficacy concerning information privacy as well as our research hypotheses. We conclude the paper with a discussion of the implications of this study and future research issues.

Self-regulation and information privacy

To study ethical decision-making pertaining to information privacy, the researcher must examine how people self-regulate themselves in stressful moral dilemmas, in which one's gain is often another's loss. The resolution of such dilemmas is not simply the choice of one outcome over the other, but may instead involve a spiral of events in which one must exercise self-control until some satisfactory resolution can be found. These control beliefs for ethical behaviors are therefore related to both objective reality and subjective mental strength. This distinguishes ethical decisions from others in that the control belief can be determined based mainly on a person's assessment of the objective reality. For example, one may believe that he or she is in full control when working in a business that has established well-defined ethical policies and procedures guarding information privacy, but at a loss when working in another organization that emphasizes efficiency and profit over professional ethics (Boatright, 1992; Headden, 1996; Resnik et al., 2000). In the latter case, the control beliefs for ethical actions fluctuate based on the relation between one's specific behavior-execution capacity and the condition of the objective reality in which that behavior takes places.

An important line of research in the domain of morality that can shed some light on this matter is Social Cognitive Theory (SCT), which adopts an interactionist perspective to moral phenomena. Within this theoretical paradigm, personal factors in the form of moral thought and affective self-reactions,

moral conduct, and environmental factors all operate as interacting determinants that influence each other bidirectionally (Bandura, 1991a). Bandura (1991a) posits that transgressive conduct is regulated by two major sources – social sanctions and internalized self-sanctions. Both control mechanisms operate anticipatorily. In control arising from social sanctions, people refrain from transgressing because they anticipate that such conduct will bring them social censure and other adverse consequences. In self-reactive control, they behave prosocially because it produces self-satisfaction and self-respect. In refraining from transgressing, people's conduct will give rise to their self-reproof.

The self-regulatory system

According to Bandura (1991b), the self-regulatory system provides the basis for purposeful action. Self-regulation is a process that is both reflective and proactive. It is regulated by both reflection and forethought: through reflecting on their past experiences, people develop their behavioral efficacy, and through the exercise of forethought, people motivate themselves and act in an anticipatory proactive way. Based on the concept of self-regulation, ethical action is not just a thing to do at a specific time and place but involves a process to constantly deal with emerging, unforeseen issues. Several ethical challenges may exist throughout this process.

First, people who conduct business as usual may not be aware that there exist discrepancies between their actions and ethical criteria. This happens because people may lack the self-regulation capacity to assess if their behaviors deviate from their espoused theories. For example, Stone (1975) and Smith (1994) studied how organizations responded to the regulations and ethical concerns that pertained to the information they handled. They found that one's actual practice was significantly different from that intended by the "spirit of the law." To some degree, these studies show the gap between ethical cognition and everyday action: knowing is one thing, doing is another. Such gaps reflect inadequate self-regulation capacity.

Second, people who encounter the dilemma may not have the conviction to make the right choices in unfavorable environmental conditions at decision time. In such situations, people become docile, despite possessing the right knowledge, when they see themselves as self-defeatists and attribute their inability to others. This may happen due to a low level of self-regulatory efficacy that, according to Bandura (1997), affects people's action strategies. A common example of a violation of information privacy is a business that uses personal data for profit, even though such use is outside the scope of the original purpose of collecting the data. For instance, an insurance company may collect and store patients' medical records for billing purposes, but later sell the data to pharmaceutical companies to market their drugs. A computer professional working for this company who becomes aware of this transaction is placed in a dilemma. Shall the professional comply with such usage, confront the top management about the transaction, or blow the whistle to outside authorities? If the professional complies, who bears the responsibility if, at a later time, the transaction is found to cause harm to certain customers? According to efficacy theory (Bandura, 1997), those whose sense of self-efficacy is high see challenges as opportunities to improve themselves, and therefore may decide to confront the management. Yet, those who are low in self-efficacy may give in to the management quickly.

Finally, even if people make the right choice and act to resolve such ethical conflicts, their effort may not be sustained because they do not possess the necessary capability or have adequate resources to actualize these decisions. This is by far the most challenging part of ethical acts: to execute the chosen course of actions in a difficult, unfavorable environment. Even though the individual has some influence over actions to achieve a certain desired outcome, many other factors governing his or her actions are beyond the individual's control. More important, the actual outcome may differ substantially from the desired outcome. The individual may therefore be required to take subsequent actions to make up for the unintended mistakes. The situation is further complicated when there are multiple sets of ethical standards that may conflict with one another. Consider the previous insurance company example, if the employee blows the whistle and the company suffers a loss in reputation, may that employee be held accountable for not being loyal (and therefore be considered unethical)? The dilemma becomes

even more challenging when the company is in a difficult financial situation, and compliance with the practice can result in great payoff for the entire company. Shall the individual resist the temptation to obey the professional ethic codes? In these cases, doing the right thing is not a simple matter of knowing but a function of an individual's self-regulation capacity.

Self-efficacy theory

Self-efficacy – the belief that one has the capability to execute a particular action – is 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). Social Cognitive Theory 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 perseverant people are in their self-controlling efforts and the greater is their success in resisting social pressures to behave in ways that violate their standards. A low sense of self-regulatory efficacy heightens vulnerability to social pressures for transgressive conduct (Bandura, 1991a, p. 69).

This research relies on Bandura's (1977) self-efficacy theory to address the question of whether male and female computer professionals differ in the self-efficacy required to protect personal information privacy. 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). In computer-related studies, several researchers have focused their attention on how computer self-efficacy expectations may impact decisions concerning technology acceptance and usage (Compeau and Higgins, 1995; Gist and Mitchell, 1992; Hill et al., 1987). Henry and Stone (1999) presented that the measures of computer self-efficacy, personal outcome expectancy, and work-related outcome expectancy display meaningful differences as a group by gender, educational level, experience in using the computer systems, and system use.

Gender differences in self-efficacy

Particularly relevant to our current endeavor are many studies that examine gender differences in self-efficacy. For example, perceived self-efficacy has been reported to mediate gender differences in performances in a variety of domains (Bandura, 1997) such as mathematics and computers. As Bandura (1997) has pointed out, these differences could be attributed to differences in the cultural practices of each gender; that is, boys are encouraged to pursue mathematics because there is a cultural expectation of ''boys should know mathematics'' but not because boys are more biologically fit than girls to study mathematics. Likewise, in many cultures the pursuit of career success is considered a necessary virtue for men but not for women, and, accordingly, breaking the rules to get what one wants may often be encouraged for the male but deemed inappropriate for the female. Throughout the world, women are in general requested to achieve higher moral standards than men in privacy-related practices (Turkle, 1988). In Taiwan, as it is in both Japan and China, women are expected to be tender and caring, and men, in contrast, are expected to pursue professional achievement. These different cultural practices may result in differences in self-regulatory efficacy between genders and, therefore, in the capacity of people to confront the ethical dilemmas that are frequently encountered in privacy-related practices.

Dimensions of self-regulatory efficacy concerning information privacy

Several studies have attempted to identify the primary dimensions of employee's concerns about organizational information privacy practices (Smith et al., 1996; Wang et al., 1998) and consumer's

attitudes toward privacy (Culnan, 1993; George, 1996). Many other studies have investigated the effectiveness of businesses' self-regulation policies and procedures (Culnan, 2000; Henderson and Snyder, 1999; Milberg et al., 1995) as well as methods for formulating privacy interface systems – the user interfaces to information protection mechanisms – for making it easy to create, inspect, modify, and monitor privacy policies (Lau et al., 1999). On the whole, most aforementioned research focuses on the issues related to organizational practice, consumers' perceptions of these practices, and societal responses. What is missing is the investigation concerning individuals' cognitive and affective capacity in sanctioning their conducts from invading others' information privacy. For this purpose, Kuo and Hsu (2001) have proposed that the employment of self-regulatory efficacy can be effective. Their study developed and tested a construct of self-regulatory efficacy concerning software piracy. This construct referred to people's perceived conviction in sanctioning their conducts from illegally copying copyrighted software. The present endeavor seeks to extend this application into the development of a measure of self-regulatory efficacy concerning information privacy.

According to Bandura (1997), self-efficacy can vary across activities and situational circumstances. Thus, there is no all-purpose measure of perceived self-efficacy scales. Rather, a scale must be tailored to a particular domain of functioning. Research evidence has also shown that the predictive capability of the self-efficacy estimate is strongest and most accurate when determined by specific domain-linked measures rather than with general measures (Bandura, 1989). Furthermore, perceived efficacy should be measured against levels of task demands that represent gradations of challenges or impediments to successful performance. The issue is not whether one can perform the activities occasionally but whether one has the efficacy to succeed in doing them regularly in the face of different types of dissuading conditions. As such, in defining self-efficacy, it is also important to consider the relevant dimensions of self-efficacy judgments. Also critical is the fact that people are asked to judge the level of their capabilities as of now, and therefore items are phrased in terms of "can do" rather than "will do." *Can* is a judgment of capability; *will* is a statement of intention. Perceived self-efficacy is a major determinant of intention.

Following the recommendation of Bandura (1997), efficacy items must be targeted to those factors over which people can exercise some control and that are related to the attainment of personal goals in the selected domain of functioning. Thus, in developing a self-regulatory efficacy instrument concerning information privacy, the initial step is to define the context from which item expressions can be written. Furthermore, one's level of self-regulatory efficacy must reveal how he or she can meet the different gradations of challenge. Accordingly, the proposed measurement must incorporate elements of task difficulty that capture differences in self-regulatory efficacy magnitude.

We therefore begin by consulting three works that reveal the dimensionality of information privacy. First, in the Privacy Protection Study Commission (PPSC, 1977), information privacy issues are classified into three categories: acquire, use, and transfer. Second, the study by Smith et al. (1996) shows that the central aspects of individuals' concerns about organizational information privacy practices are collection of personal information, internal unauthorized secondary use of personal information, external unauthorized secondary use of personal information, error in personal information, and improper access to personal information. Finally, Wang et al. (1998) have made a taxonomy for information privacy concerns: improper acquisition (improper access, improper collection, improper monitoring); improper use (improper analysis, improper transfer); privacy invasion (unwanted solicitation); and improper storage.

To summarize the previous classifications in information privacy, privacy invasion behavior can be conceptually divided into three dimensions: protection, non-distribution, and non-acquisition. *Protection* refers to whether an individual can take the necessary courses of action for guarding accidental disclosures of information in a public environment. This dimension includes improper use (PPSC, 1977; Smith et al., 1996), improper monitoring (Wang et al., 1998), privacy invasion (Wang et al., 1998), and improper storage (Wang et al., 1998). *Non-distribution* refers to whether a person can exert his or her control not to distribute the privacy information of others, which includes

TABLE I

Dimensions of information privacy self-regulatory efficacy

Source	Dimension (challenge level)		
	Protection	Non-distribution	Non-acquisition
Privacy Protection Study Commission (1977)	Improper use	Improper transfer	Improper acquisition
Smith et al. (1996)	Improper use	Internal/external unauthorized secondary use	Improper collection
Wang et al. (1998)	Improper monitoring Privacy invasion Improper storage	Improper transfer	Improper access Improper collection Improper analysis

Protection: One's perception of efficacy in protecting others' privacy information.
Non-distribution: One's perception of efficacy in sanctioning against distributing the privacy information of others.
Non-acquisition: One's perception of efficacy in sanctioning against acquiring the privacy information from others.

improper transfer (PPSC, 1977; Wang et al., 1998), and internal/external unauthorized secondary use (Smith et al., 1996). *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. This dimension includes improper collection (Smith et al., 1996; Wang et al., 1998), improper acquisition (PPSC, 1977), improper access (Wang et al., 1998), and improper analysis (Wang et al., 1998). Table I presents a brief summary of these three dimensions.

Research hypotheses

In virtually all societies of our world, different groups of people are assigned different roles and given different expectations based on the characteristics of their traits and/or the tasks they perform. Consequently, each group would form its own subculture that may differ substantially from others. In fact, Bandura (1997) himself has posited that efficacy beliefs are derived mainly from direct experience, vicarious observation, and verbal persuasion. As a result, different groups' particular cultural practices concerning morality should also result in differences in perceived self-efficacy of moral self-regulation. Indeed, in moral conducts involving computer uses, the phenomena of cultural differences have been reported. A survey by Kerie and Cronan (1998), for example, showed that gender differences exist between men and women in their assessment of which behaviors were ethical and which were not. In the five scenarios of making unauthorized copies of programs, Kerie and Cronan found that men were less likely than women to consider piracy as unethical. Moreover, men's judgments were most often influenced by their personal values and one environmental cue – whether the action was legal. Conversely, women were found to be more conservative in their judgments and they considered more environmental cues than men.

Note that the ability to observe environmental cues in one's decision is an important factor in forming efficacy beliefs, which, according to SCT (Bandura 1986, 1997), are strongly influenced by vicarious observation and verbal persuasion. In this theory, people learn by observing the performance of referent peers and by evaluating the feedback they receive for their actions. This learning may, in turn, lead to the strengthening or weakening of self-regulatory efficacy. In the case of ethical practices, by being able to effectively incorporate these environmental factors, women can make better ethical judgments than men. Similarly, Gattiker and Kelly (1999) further demonstrated that men and women indeed differ in their judgments of consequences pertaining to the moral domain. Using a vignette involving the use of computer technology to access and distribute a banned game containing unethical materials, these authors discovered that women were more careful about how their actions might affect others. Therefore, we hypothesize first that, in the area of information privacy, women have a higher level of self-regulatory efficacy than men:

Hypotheses 1: Females will demonstrate a higher level of self-regulatory efficacy concerning information privacy than males.

In addition, Gattiker and Kelly (1999) concluded that, in general, women's use of IS followed prevailing societal norms and cultures more than that of men. Thus, we hypothesize that women's levels of self-regulatory efficacy in all three dimensions would be higher than those of men. The following three hypotheses are therefore proposed.

Hypotheses 2: Females will demonstrate higher self-regulatory efficacy in their *protection* of information privacy than males.

Hypotheses 3: Females will demonstrate higher self-regulatory efficacy in their *non-distribution* of information privacy than males.

Hypotheses 4: Females will demonstrate higher self-regulatory efficacy in their *non-acquisition* of information privacy than males.

The measurement

The dimensions of information privacy self-regulatory efficacy, shown in Table I, becomes the basis of an iterative process to generate a sample of items from which the content validity can be assessed. During this process, scale items can be trimmed and refined; and dimensions may be added, deleted, or modified as the understanding of the construct improves. In our study, several means were used to accomplish this goal: literature reviews, focus groups, expert judges, and pilot testing with relevant samples (Smith et al., 1996). After several rounds of domain development and refinement, an initial set of 13 instruments was developed by a group of three experts (see Table II).

Each expert agreed that this set of items captured relevant underlying dimensions for measuring people's perceived efficacy in protecting information privacy. To consolidate redundancies, a pilot test was administered to 141 students and an exploratory factor analysis was conducted. The result showed three principal factors: *Protection, non-distribution*, and *non-acquisition* (see Table III). This confirmed the previous classification in information privacy. Furthermore, among the 13 items, the item 4 (*P4*) in the Protection dimension, was eliminated due to its high correlation (>0.90) with the item 3 (*P3*); the item 1 (*P1*) was eliminated for ineligible loading; and the item 1 (*D1*) in the Non-distribution dimension was eliminated to increase the construct reliability. Note that no two items have a correlation greater than 0.90. The revised scale consisted of 10 items, reflecting the interrelated self-efficacy dimensions, which are themselves measured by multiple indicators.

Note that an effective instrument for measuring self-regulatory efficacy must include different levels of challenges for each dimension. In our proposed construct, this is accomplished by differentiating the level of gradations for the specific target behavior. The efficacy scale is unipolar, ranging from 0 to a maximum strength of 10 or 100. The Privacy Self-Regulatory Efficacy scale in this study consists of 10 intervals ranging from 0 (''Cannot do'') to complete assurance 100 (''Can certainly do''). Such scales can reveal both magnitude (can or cannot do an activity of a certain difficulty) and strength (level of conviction in doing that activity). Scores for the three efficacy subscales were obtained by summing items on each subscale.

Results

Subjects

A total of 180 surveys were sent to the IS managers or senior computer professionals in 30 companies in Taiwan. Each IS manager or senior computer professionals was asked to distribute six surveys to individuals who agreed to participate voluntarily in the study. Participants were told that their responses would be kept confidential and that only summary information would be presented. A total of 175 surveys were returned. The exclusion of incomplete questionnaires resulted in a total of 168 usable

TABLE II

Initial instruments for information privacy self-regulatory efficacy

Items	Instrument
Protection	
P1⋆	If you happen to find your colleagues viewing some information concerning the privacy of customers, how confident are you to try to dissuade them from viewing it?
P2	If you happen to find your colleagues copying some information concerning the privacy of customers, how confident are you to try to dissuade them from copying it?
P3	If you happen to find that some customers? privacy information is revealed on the network, how confident are you to protect this information immediately?
P4⋆	If you happen to find that your colleagues are revealing some customers? privacy information on the network, how confident are you to try to dissuade them from revealing it?
Non-distribution	
D1⋆	If your colleagues ask you to share some customers? privacy information that you own, how confident are you to refuse to share the information with them?
D2	If your colleagues badly need some customers? privacy information that you own, how confident are you to refuse to share the information with them?
D3	If your colleagues want to purchase some customers? privacy information that you own, how confident are you to refuse to grant the request?
Non-acquisition	
A1	If you have the opportunity to analyze the privacy information concerning your customers beyond the original purpose, how confident are you not to take advantage of this situation?
A2	If you are approached by the collaborator who has a need to analyze privacy information concerning your customers beyond the original purpose, how confident are you not to take advantage of this situation?
A3	If, without others knowing, you are able to keep some information concerning the privacy of your customers, how confident are you not to take advantage of this situation?
A4	If, without others knowing, you are able to gather some information concerning the privacy of customers who belong to other companies, how confident are you not to gather this information?
A5	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?
A6	If, without others knowing, you are able to access some information concerning the privacy of the customers via the Internet, how confident are you not to take advantage of this situation?

⋆P1 was eliminated due to the ineligible loading. P4 was eliminated due to high correlation (>0.90) with P3. D1 was eliminated to increase the construct reliability of ''non-distribution.'' The revised self-regulatory efficacy scales consisted of 10 items.

responses (a net response rate of 93%). Among the respondents, 103 were males and 65 were females. Respondents had an average work experience of 12 years, and their average age was 35 years.

Table IV summarizes the demographic characteristics of the respondents. A recent survey on human resources in Taiwan indicated that in the past 3 years, about 43% of technology professionals are female (http://www.dgbas.gov.tw/census~n/four/yt3a.htm). Since 39% of the subjects in this study are female, we consider the results of this study to have adequate generalizability.

Reliability and validity assessment

Table V shows the descriptive statistics and reliabilities among the research variables. The reliability of each multiple-item measure is estimated using composite reliability, a commonly used measure of internal consistency. The results show that the value was 0.896 for the *protection* factor, 0.836 for the *non-distribution* factor, and 0.941 for the *non-acquisition* factor. All variables in the present research are greater than 0.7, indicating that the measures are reliable (Tull and Hawkins, 1993).

TABLE III

Factor structure matrix

	Component		
	Non-acquisition	Non-distribution	Protection
A1	0.637	0.169	0.254
A2	0.690	0.144	0.012
A3	0.634	0.236	0.278
A4	0.640	0.375	0.250
A5	0.546	0.173	0.123
A6	0.560	0.228	0.307
P2	0.392	0.539	0.260
P3	0.273	0.935	0.215
D2	0.138	0.178	0.972
D3	0.235	0.172	0.480

Factor Analysis by LISREL.
Rotation Method: Varimax-Rotated.

TABLE IV

Sample demographics

Demographic variable	Sample composition
Age	Mean = 35; Range: 29–48
Gender	61% Male 39% Female
Years of work experience	Mean = 12; Range:5–22
Major	46% Programmer 24% System analyst 20% Database administrator 10% System maintainer

In validation of the variables, convergent validity and discriminant validity were assessed. Table V shows that all factor loadings are greater than 0.5 and all are statistically significant at $p < 0.01$. This implies that the measures satisfy convergent validity. In addition, convergent validity can be assessed in terms of the degree to which the subscales are correlated (Barki and Harwick, 1994). The matrix in Table VI provides strong evidence of convergent validity with regard to the efficacy subscales (protection, non-distribution, and non-acquisition efficacy). The correlation between all the dimensions is significantly different at $p < 0.01$.

Discriminant validity can be observed through comparison of the average variance extracted for construct pairs to the squared correlation between pairs. Table VI shows that the average variance extracted for all constructs is well above the correlation among constructs, indicating that the measure has high discriminant validity (Fornell and Larcker, 1981). Therefore, we conclude that the measures satisfy construct validity. Furthermore, Figure 1 shows that the measurement of Information Privacy Self-Regulatory Efficacy is an aggregate of three dimensions: protect access to customers' privacy information (standardized coefficient = 0.87, $p < 0.01$); (2) not distribute the privacy information to any third party or

TABLE V

Descriptive statistics and reliability for the study variables

Construct	Item	Mean	Standard deviation	Standardized factor loading	Composite reliability*
Protection	P2	1.51	2.01	0.80	0.896
	P3	1.89	2.05	0.83	
Non-distribution	D2	3.94	2.58	0.80	0.836
	D3	3.39	2.71	0.66	
Non-acquisition	A1	2.57	2.01	0.68	0.941
	A2	2.45	2.27	0.61	
	A3	2.28	2.14	0.72	
	A4	1.80	1.85	0.80	
	A5	2.87	2.84	0.58	
	A6	1.74	2.19	0.69	

*Composite reliability = $(\sum \mathrm{Li})^2/((\sum \mathrm{Li})^2 + \sum \mathrm{Var(Ei)})$.

TABLE VI

Discriminant validity for the study variables

Construct	Protection	Non-distribution	Non-acquisition
Protection	0.809		
Non-distribution	0.391	0.725	
Non-acquisition	0.607	0.507	0.733

1. All correlations are significant at the 0.01 level (2-tailed).
2. Diagonal elements represent the Average Variance Extracted (AVE), and off-diagonal elements represent the correlations among constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements.
3. Average Variance Extracted = $(\sum Li)^2/((\sum Li)^2 + \sum Var(Ei))$Average Variance Extracted recommended value (Fornell and Larcker, 1981): >0.50.

for one's personal use (standardized coefficient = 0.71, $p < 0.01$); and (3) not acquire privacy information for undisclosed purposes (standardized coefficient = 0.87, $p < 0.01$). The resulting measure therefore is a 10-item instrument that can be operationalized as a second-order factor model, in which a latent factor (i.e., information privacy self-regulatory efficacy) governs the correlations among *protection, non-distribution*, and *non-acquisition*.

Hypotheses testing

Mean scores are determined for male and female respondents along the three dimensions and over all of the measures. A one-way ANOVA method is employed to test the hypotheses by determining whether real differences exist between these means. These results are reported in Table VII. Due to the unequal sizes of the two gender groups, it is

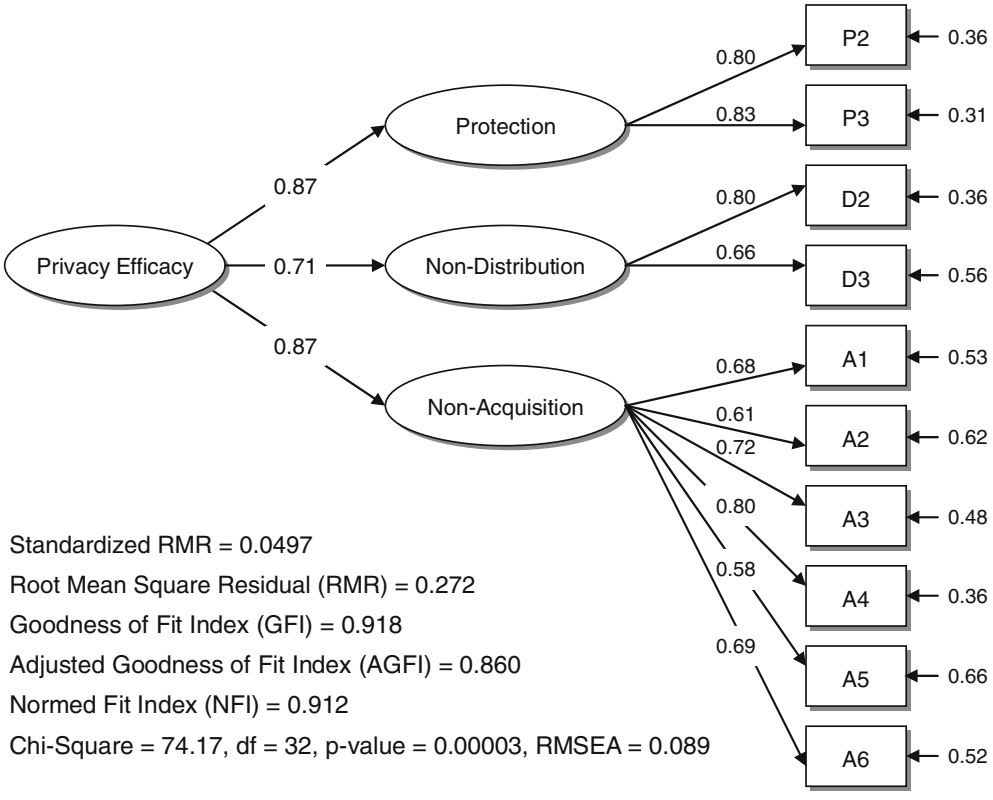

Figure 1. Second-order model of self-regulatory efficacy concerning information privacy.

TABLE VII
Hypotheses test

Construct	Male ean score	Female mean score	*F*-value	Sig.	Hypotheses support
SE_ALL	2.40	3.17	10.18	0.002**	Yes
Protection	1.31	2.32	12.66	0.000**	Yes
Non-distribution	3.99	4.32	0.87	0.353	No
Non-acquisition	1.91	2.88	14.81	0.000**	Yes

Statically significant parameters: $^{**}p < 0.05$.

necessary to test the homogeneity of variance to determine if the unequal size poses a problem to the ANOVA test. The results of testing the homogeneity of variance show that there is no significant difference between the two gender groups at the 0.01 level.

As shown in Table VII, female subjects exhibit a higher score than male subjects in the overall self-regulatory efficacy concerning information privacy. Female subjects also perform better than males in two out of three dimensions of information privacy – *protection* and *non-acquisition*, but no significant difference can be found between males and females in the *non-distribution* dimension. This implies that female subjects in this study possess a higher level of self-regulatory efficacy concerning the protection and non-acquisition of personal privacy information. Thus, the ANOVA results support the first hypo-thesis ($F = 10.18$, $p < 0.05$), the second hypothesis ($F = 12.66$, $p < 0.05$), and the fourth hypothesis ($F = 14.81$, $p < 0.05$), but not the third hypothesis.

Discussions and conclusions

In this study, an instrument of self-regulatory efficacy concerning information privacy has been developed based on the self-regulatory efficacy theory. The result is a 10-item instrument with three subscales (*protection, non-distribution*, and *non-acquisition*) tapping into dimensions of individuals' self-regulatory efficacy concerning personal information privacy. The development of such multidimensional conceptualizations can capture the multiple aspects of the measure that may be subsumed within a general (single-scale) measure. It also provides insight into the nature of interrelationships among self-regulatory efficacy dimensions.

This development is important because little attention has been paid to instrumentation issues in information ethics research (Smith et al., 1996). Now, through examining the factorial structure of the individuals' self-regulatory efficacy concerning information privacy, researchers can undertake studies to carefully examine the links of its subscales to such variables as ethical attitude, ethical intention, self-esteem, and self-sanction, which are considered important in one's ethical decisions related to information privacy. Studies can also be extended to investigate how different cultural practices of morality and computer use in men and women may shape the different development patterns of privacy self-efficacy. As Adam et al. (2004) have suggested, researchers need to treat gender as a cultural variable rather than some fixed, unchangeable characteristic. Understanding the different cultural practices may then shed light on the social sources of privacy competence and the appropriate remedies that can be provided to improve the situation.

This study shows that the female computer professionals in this study demonstrated a higher level of self-regulatory efficacy in the domains of ''protection" and ''non-acquisition". Note that according to the efficacy theory, the specific domain of efficacy may vary due to demographic or situational differences. Therefore, a different result is possible for other studies that sample different subject populations. Critical to the current endeavor is the result of our study, conducted in Taiwan, that female computer professionals demonstrate a higher level than their male counterparts of the overall

self-regulatory efficacy concerning privacy, which appears to be consistent with the results of several prior studies in the Western context that show females tend to act more ethically than males in dealing with ethical challenges in general (Beltramini et al., 1984; Chonko and Hunt, 1985; Ferrell and Skinner, 1988; Jones and Gautschi, 1988; Kidwell et al., 1987; Reiss and Mitra, 1998; Ruegger and King, 1992; Whipple and Swords, 1992) and in the protection of privacy in particular (Sheehan, 1999; Westin, 1997).

Considering that there exists a significant gap in the cultural practices of morality and computer use in men and women, the self-efficacy beliefs concerning self-regulation of information privacy should also vary between men and women. The differential cultural ethical conceptions therefore facilitate the female to display a relatively more rigorous self-regulatory capacity than the male in privacy-related practices. Understanding this female strength in self-regulatory capacity concerning privacy is important in dealing with the growing number of privacy-related dilemmas that confront computer professionals today.

The computer-related workplace, which according to Turkle (1988), has been socially constructed as a male-dominant culture, often emphasizes technology over people. It tends to praise masculine properties such as achievement, eminence, accomplishment, and assertiveness over feminine attributes such as affiliation, person-orientation, empathy, and collective actions. Yet, in the technology-based society in which people are virtually interconnected in one way or another, the feminine properties have become increasingly more important to ensure fairness and justice to all people. Thus, in the immediate future, a rise in the presence of the female computer-related workforce could be beneficial to confront the ever-increasing ethical problems in workplaces in which the application of IT has increased dramatically in the last two decades. Although increasing the numbers of females in the IT workforce is not the answer to all ethical problems related to IT application, such an increase would certainly improve the many careless practices that may harm privacy. Furthermore, placing people with the properties of person-orientation and collective actions (deemed feminine properties) in key managerial positions may exert a great impact. For example, this person should be the leading member of the committee that formulates privacy policies and periodically reviews employees' ethical practices. Also, ethical codes reflecting masculine and feminine differences in privacy practices should be established to guide IT professionals in self-regulating their conduct.

In addition, self-efficacy safeguarding privacy should not be treated as an invariant trait of the female but rather a competence that can be developed through the social learning process. In line with the contention of Bandura (1997), experiences gained through cultural practices are important sources of self-efficacy; and the orientation toward ''collective social group responsibility'' should be attributed to differences in the cultural practices of each gender. As cultural practices are altered, men may develop similar orientations. Thus, in the long run, education that fosters person-orientation, empathy, and collective actions can be provided to people to ensure the development of a high level of privacy self-efficacy. Such gender-sensitive ethical education can also be integrated into IS curricula so students will possess the self-regulatory capacity needed to secure our technological society. These various means may then serve to safeguard the social fabric that is essential to ensure the satisfaction of people as IT progresses.

Limitations

According to the Social Cognitive Theory, self-efficacy is highly dependent on the domain of functioning and the situational differences. As a result, replicating this survey at a later date or in different cultures may yield different results. Furthermore, the findings of this study should not be generalized to the entire population of computer professionals around the world without significant additional testing of the cultures of different populations. Future works can be conducted to examine how situational differences may impact the level of privacy self-efficacy and how the impact may differ in different cultures. Finally, due to the sensitive nature of the issue of privacy, subjects may not have answered the survey in complete honesty. In situations as such, subjects may answer the survey in a manner that heightens social approval instead of

reflecting one's true feelings (Crowne and Marlowe, 1960; Paulhus, 1991). Future studies should therefore take this social desirability tendency into consideration so as to reduce possible bias.

Acknowledgements

This research is sponsored by the NSC of Taiwan, grant no. NSC 92-2416-H-110-016 and NSC 92-2416-H-390-007.

References

Adam, A.: 2000, 'Gender and Computer Ethics', *Computers and Society* December, 17–24.

Adam, A., D. Howcroft and H. Richardson: 2004, 'A Decade of Neglect: Reflecting on Gender and IS', *New Technology, Work and Employment* **19**(3), 222–240.

Bandura, A.: 1977, 'Self-efficacy: Toward a Unifying Theory of Behavioral Change', *Psychological Review* **84**(1), 191–215.

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

Bandura, A.: 1989, 'Regulation of Cognitive Processes through Perceived Self-Efficacy', *Development Psychology* **25**(5), 729–735.

Bandura, A.: 1991a, 'Social Cognitive Theory of Moral Thought and Action', in W. M. Kurtines and J. L. Gewirtz (eds.), *Handbook of Moral Behavior and Development 1* (Erlbaum, Hillsdale, NJ), pp. 45–103.

Bandura, A.: 1991b, 'Social Cognitive Theory of Self-Regulation', *Organizational Behavior and Human Decision Processes* **50**, 248–287.

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

Barki, H. and J. Harwick: 1994, 'Measuring User Participation, User Involvement, and User Attitude', *MIS Quarterly* **18**(1), 53–63.

Beltramini, R. F., R. F. Peterson and G. Kozetsky: 1984, 'Concerns of College Students Regarding Business Ethics', *Journal of Business Ethics* **3**, 195–200.

Bissett, A. and G. Shipton: 1999 'An Investigation into Gender Differences in the Ethical Attitudes of IT Professionals', ETHICOMP99, Rome, October.

Boatright, J.: 1992, 'Conflict of Interest: An Agency Analysis', in N. Bowie and R. Freedman (eds.), *Ethics and Agency Theory: Introduction* (Oxford University Press, New York), pp. 187–203.

Chonko, L. B. and S. Hunt: 1985, 'Ethics and Marketing Management: An Empirical Investigation', *Journal of Business Research* **13**, 339–359.

Compeau, D. R. and C. A. Higgins: 1995, 'Computer Self–Efficacy: Development of a Measure and Initial Test', *MIS Quarterly* **19**(2), 189–211.

Crowne, D. P. and D. Marlowe: 1960, 'A New Scale of Social Desirability Independent of Psychopathology', *Journal of Consulting Psychology* **24**, 349–354.

Culnan, M.: 1993, 'How Did You Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use', *MIS Quarterly* **17**(3), 341–361.

Culnan, M. J.: 2000, 'Protecting Privacy Online: Is Self-Regulation Working?', *Journal of Public Policy and Marketing* **19**(1), 20–26.

Dawson, L. M.: 1997, 'Will Feminization Change the Ethics of the Sales Profession?', *Journal of Personal Selling and Sales Management* **12**, 21–32.

Escribano, J. J., R. Pena and J. Extremera: 1999, 'Differences between Men and Women in Terms of Usage and Assessment of Information Technologies', ETHICOMP99, Rome, October.

Ferrell, O. C. and S. J. Skinner: 1988, 'Ethical Behavior and Bureaucratic Structure in Marketing Research Organizations', *Journal of Marketing Research* **25**(1), 103–109.

Fornell, O. C. and D. F. Larcker: 1981, 'Evaluating Structural Equation Models with Unobservable and Measurement Error', *Journal of Marketing Research* **18**, 39–50.

Gattiker, U. E. and H. Kelly: 1999, 'Morality and Computers: Attitudes and Differences in Moral Judgments', *Information Systems Research* **10**(3), 233–254.

George, J. F.: 1996, 'Computer-Based Monitoring: Common Perceptions and Empirical Results', *MIS Quarterly* **20**(4), 459–480.

Georgia Tech Research Corporation, WWW User Survey, 7th Survey in (1997), 10th Survey in 1998, available at http://www.cc.gatech.edu/gvu/user_surveys/.

Gist, M. E. and T. R. Mitchell: 1992, 'Self-Efficacy: A Theoretical Analysis of Its Determinants and Malleability', *Academy of Management Review* **17**(2), 183–211.

Harrington, S. J.: 1995, 'Computer Crime and Abuse by IS Employees', *Journal of Systems Management* March/April, 6–11.

Headden, S.: 1996, Danger at the Drugstore. U.S. News and World Report (26 August 1996), pp. 46–53.

Henderson, S. C. and C. A. Snyder: 1999, 'Personal Information Privacy: Implications for MIS Managers', *Information and Management* **36**, 213–220.

Henry, J. W. and R. W. Stone: 1999, 'The Impacts of End-User Gender, Education, Performance, and System Use on Computer Self-Efficacy and Outcome Expectancy', *Southern Business Review* **25**(1), 10–16.

Hill, T., N. D. Smith and M. F. Mann: 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.

Jones, T. M. and F. H. Gautschi: 1988, 'Will the Ethics of Business Change? A Survey of Future Executive', *Journal of Business Ethics* **7**, 231–248.

Kerie, J. and T. P. Cronan: 1998, 'How Men and Women View Ethics', *Communication of the ACM* **41**(9), 70–76.

Khazanchi, D.: 1995, 'Unethical Behavior in Information Systems: The Gender Factor', *Journal of Business Ethics* **14**, 741–749.

Kidwell, J. M., R. E. Stevens and A. L. Bethke: 1987, 'Differences in Ethical Perceptions between Male and Female Managers: Myth or Reality', *Journal of Business Ethics* **6**, 489–493.

Kuo, F. Y. and M. H. Hsu: 2001, 'Development and Validation of Ethical Computer Self-Efficacy Measure: The Case of Softlifting', *Journal of Business Ethics* **32**, 299–315.

Latham, G. P. and C. A. Frayne: 1989, 'Self-Management Training for Increasing Job Attendance: A Follow-up and a Replication', *Journal of Applied Psychology* **74**, 411–416.

Lau, T., O. Oren Etzioni and D. S. Weld: 1999, 'Privacy Interfaces for Information Management', *Communication of the ACM* **42**(10), 89–94.

Loch, K. D. and S. Conger: 1996, 'Evaluating Ethical Decision Making and Computer Use', *Communications of the ACM* **39**(7), 74–83.

Marakas, G. M., M. Y. Yi and R. D. Johnson: 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), 126–163.

Mason, E. S. and P. E. Mudrack: 1996, 'Gender and Ethical Orientation: A Test of Gender and Occupational Socialization Theories', *Journal of Business Ethics* **15**, 599–604.

Mason, R. O.: 1986, 'Four Ethical Issues of the Information Age', *MIS Quarterly* **10**(1), 5–12.

Milberg, S. J., S. J. Burke, J. Smith and E. A. Kallman: 1995, 'Values, Personal Information Privacy, and Regulatory Approaches', *Communications of the ACM* **38**(12), 65–74.

Oz, E.: 1992, 'Ethical Standards for Information System Professionals: A Case for a Unified Code', *MIS Quarterly* 423–433.

Panteli, A., J. Stack, M. Atkinson and H. Ramsay: 1999a, 'The Status of Women in the UK IT Industry: An Empirical Study', *European Journal of Information Systems* **8**, 170–182.

Panteli, A., J. Stack and H. Ramsay: 1999, 'Gender and Professional Ethics in the IT Industry', *Journal of Business Ethics* **22**(1), 51–61.

Panteli, N., J. Stack and H. Ramsay: 2001, 'Gendered Patterns in Computing Work in the Late 1990s', *New Technology, Work and Employment* **16**(1), 3–17.

Paulhus, D. L.: 1991, 'Measurement and Control of Response Bias', in J. P. Robinson, P. Shaver and L. S. Wrightsman (eds.), *Measures of Personality and Social Psychological Attitudes* (Academic Press, San Diego), pp. 17–59.

PPSC (Privacy Protection Study Commission): 1977, *Personal Privacy in an Information Society: Report of the Privacy Protection Study Commission* (U.S. Government Printing Office, Washington, DC.).

Privacy and American Business, Commerce, Communication and Privacy Online: A National Survey of Computer Users (1997) (Hackensack, NJ: Privacy and American Business).

Radtke, R. R.: 2000, 'The Effects of Gender and Setting on Accountants' Ethically Sensitive Decisions', *Journal of Business Ethics* **24**, 299–312.

Reiss, M. C. and K. Mitra: 1998, 'The Effects of Individual Difference Factors on the Acceptability of Ethical and Unethical Workplace Behaviors', *Journal of Business Ethics* **17**(14), 1581–1593.

Resnik, D. B., P. L. Ranelli and S. P. Resnik: 2000, 'The Conflict Between Ethics and Business in Community Pharmacy: What about Patient Counseling?', *Journal of Business Ethics* **28**, 179–186.

Robertson, M., S. Newell, J. Swan, L. Mathiassen and G. Bjerknes: 2001, 'The Issue of Gender within Computing: Reflections from the UK and Scandinavia', *Information Systems Journal* **11**, 111–126.

Ruegger, D. and E. W. King: 1992, 'A Study of the Effect of Age and Gender upon Student Business Ethics', *Journal of Business Ethics* **11**, 179–186.

Sheehan, K. B.: 1999, 'An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors', *Journal of Interactive Marketing* **13**, 24–38.

Smith, H. J., S. J. Milberg and S. J. Burke: 1996, 'Information Privacy: Measuring Individuals' Concerns about Organizational Practices', *MIS Quarterly* **20**(2), 167–196.

Smith, H. J.: 1994, *Managing Privacy: Information Technology and Corporate America* (University of North Carolina Press, Chapel Hill).

Stone, C. D.: 1975, *Where the Law Ends: The Social Control of Corporate Behavior* (Harper & Row, New York).

Truman, G. E. and J. J. Baroudi: 1994, 'Gender Differences in the Information Systems Managerial Ranks: An Assessment of Potential Discriminatory Practices', *MIS Quarterly* June, 129–142.

Tull, D. S. and D. I. Hawkins: 1993, *Marketing Research: Measurement and Method* (Macmillan, New York.).

Turkle, S.: 1988, 'Computational Reticence: Why Women Fear the Intimate Machine', in Kramarae (eds.), *Technology and Women's Voices: Keeping in Touch* (Pergamon Press, Oxford, UK).

Wang, H., M. Lee and C. Wang: 1998, 'Consumer Privacy Concerns about Internet Marketing', *Communication of the ACM* **41**(3), 63–70.

Westin, A. F.: 1997, *Commerce, Communication, and Privacy Online* (Center for Social and Legal Research, Hackensack, NJ).

Whipple, T. W. and D. F. Swords: 1992, 'Business Ethics Judgment: A Cross Cultural Comparison', *Journal of Business Ethics* **11**, 671–678.

F.-Y. Kuo
Department of Information Management, National Sun Yat-Sen University, Kaohsiung, 804, Taiwan

C. S. Lin
Department of Information Management, National University of Kaohsiung, Kaohsiung, 811, Taiwan
E-mail: cathy@nuk.edu.tw

Meng-Hsiang Hsu
Department of Information Management, National Kaohsiung of First University of Science and Technology, Kaohsiung, 811, Taiwan