Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens

—SANGMI CHAI, SHARMISTHA BAGCHI-SEN, CLAUDIA MORRELL, H. R. RAO, AND SHAMBHU J. UPADHYAYA, SENIOR MEMBER, IEEE

***Abstract*—*Information security and privacy on the internet are critical issues in our society. In this research, we examine factors that influence internet users' private-information-sharing behavior. Based on a survey of 285 preteens and early teens, who are among the most vulnerable groups on the web, this study provides a research framework that explains an internet user's information privacy protection behavior. According to our study results, internet users' information privacy behaviors are affected by two significant factors: (1) users' perceived importance of information privacy and (2) information privacy self-efficacy. The study also found that users believe in the value of online information privacy and that information privacy protection behavior varies by gender. Our findings indicate that educational opportunities regarding internet privacy and computer security as well as concerns from other reference groups (e.g., peer, teacher, and parents) play an important role in positively affecting the internet users' protective behavior regarding online privacy.*

***Index Terms*—*Information privacy anxiety (IPA), information privacy protection behavior (IPPB), online information privacy, protection motivation theory, self-efficacy, Social Cognitive Theory.*

Information privacy is defined as "the claim of individuals, groups, or institutions to determine of themselves when, how, and to what extent information about them is communicated to others" [1, p. 7]. While information and communication technology deliver various benefits to our daily life, increasing threats in cyberspace and online information privacy breaches are two growing, critical problems. While advances in computer technology increase access to personal information, this increasing access can jeopardize individuals' information privacy [2]. For the organizations, monitoring workers' email content was also discussed as an issue regarding legal and ethical concerns in the workplace [3]. Computer technology and communication bring an obvious advantage to individuals, organizations, and schools by conferring on them easy and fast access to the world of information. While the internet becomes an important source of entertainment, commerce, and education, online users are facing more possibilities of online privacy breaches and cyber crimes, which lead to growing public concern about online information privacy. However, the rapid development of information technology (IT) can make even the most aware users vulnerable.

While more than three-quarters of American consumers expressed highly intensive information privacy concerns in 2001 [4], companies want to collect and use online consumers' more personal information for marketing and strategic purposes. Moreover, technology facilitates an organization's ability to collect online users' personal information easily and without immediate recognition by online users by using cookies and tracking software [5].

According to the Federal Trade Commission, 85% of the sites that consumers had visited collected personal information from them, whereas only 14% had posted any privacy-related notices [6]. Public concerns about online privacy lead the government's efforts to protect online users from a possible information privacy breach. Beginning with the data protection directive of the European Union in 1995, the US Congress enacted the Children's Online Privacy Protection Act in 1998 to regulate the online collection and use of personal information from children, who are one of the most vulnerable groups in online information privacy. The US Congress also passed The Gramm–Leach–Bliley Act to protect personal information privacy in the financial industry in 1999.

Even though continuous efforts are expended to prevent the illegal acquisition and use of personal information on the web, information privacy and security threats are increasing rapidly in cyberspace. Effective protection for groups whose information privacy is vulnerable is a particularly

Manuscript received August 27, 2007; revised January 15, 2008. Current version published May 20, 2009.
S. Chai, S. Bagchi-Sen, H. R. Rao, and S. J. Upadhyaya are with the State University of New York at Buffalo, Buffalo, NY 14260 USA (email: schai2@buffalo.edu; geosbs@buffalo.edu; mgmtrao@buffalo.edu; shambhu@cse.buffalo.edu).
C. Morrell is with the Multinational Development of Women in Technology (MDWIT), Baltimore, MD 21234 USA (email: cmorrell@mdwit.org).
IEEE 10.1109/TPC.2009.2017985

important, emerging issue in our society. Children and teenagers, two of the most vulnerable groups on the internet, compose the largest portion of internet users in the US. Indeed, 65% of children between the ages of 10 and 13 use the internet [7]. Research shows that 163 out of 166 websites collect personal information from children without any effort to elicit parental involvement, even after the enactment of the Children's Online Privacy Protection Act [8]. Reported computer crimes that are related to online privacy breaches and incidents involving teenagers, such as social engineering, phishing, bullying, and harassment, are exponentially escalating [9].

However, as Turow's study shows, most online users do not know how to protect their personal information on the web. According to that study's survey results, 64% of 1,200 online users responded that they never searched for information about how to protect information on the web, and 40% of adult users who use the internet at home said that they know "almost nothing" about preventing sites from collecting information about them [10, p. 3].

From these findings, we can conclude that regulation and institutional efforts are not enough to protect online users from online privacy incidents. Within the online community, children and teenagers are the fastest growing group. In addition, they are very vulnerable to cybercrimes originating from information privacy breaches, cyber stalking, online sexual harassment, and cyber bullying [9]. Children can be easily convinced to share their personal information with the promise of a small prize or gift [11]. Since children and teenagers tend to be trusting, naïve, curious, adventuresome, and eager for attention and affection, potential offenders and strangers have found that children and teenagers are perfect targets for criminal acts in cyberspace [12]. Despite the importance and vulnerability of this demographic group, this subset of the community has hardly been researched in the context of cybersecurity. In this research, we focus on online users' behavior regarding online privacy, specifically focusing on preteens and early teens (i.e., those who are just entering their teen years).

In our research, we empirically explored the factors that influence the internet user's personal-information-sharing behavior on the internet. In addition, we investigated gender differences as perceptions of the importance of internet privacy and information privacy protection behavior (IPPB).

To discover the answers of our research objectives, we carried out an empirical study of middle school students who are familiar with IT and the internet environment (yet, they are one of the vulnerable groups in the context of online privacy). We use Social Cognitive Theory and Protection Motivation Theory to understand internet users' IPPB. We develop a model that incorporates information privacy self-efficacy, perceived information privacy importance, and information privacy exposure as important factors in influencing attitudes toward information privacy.

THEORETICAL DEVELOPMENT

In this subsection, we discuss the two theories that are the drivers of our research model: the Social Cognitive Theory that has been proposed by Bandura [13] and the Protection Motivation Theory primarily ascribed to Rogers [14].

Social Cognitive Theory Social Cognitive Theory is widely used to explain individual behavior. It premises that personal factors in the form of cognitive, affective, and biological events, as well as behavioral and environmental events, all operate as interacting determinants that influence each other [13]. According to this theory, individuals choose the environment in which they exist and are influenced by that environment. Furthermore, behavior in a given situation and the environment affect each other. Finally, behavior is influenced by cognitive and personal factors [15]. According to Bandura, in this reciprocal relationship among environment, behavior, and the individual, self-efficacy is a major cognitive force guiding individual behavior. He defines self-efficacy as a person's judgment of his or her capabilities to perform a task. Self-efficacy is concerned with judgments of what one can or cannot do with skills [13].

In the context of IT, the research suggests that individuals who possess high self-efficacy toward IT use IT more frequently [16]. People who have a higher level of self-efficacy toward a specific subject are more likely to give greater value to that subject. In our research, we use Social Cognitive Theory as a key theoretical background.

Protection Motivation Theory Protection Motivation Theory provides a conceptual framework to understand fear appeal and behavioral change [14].

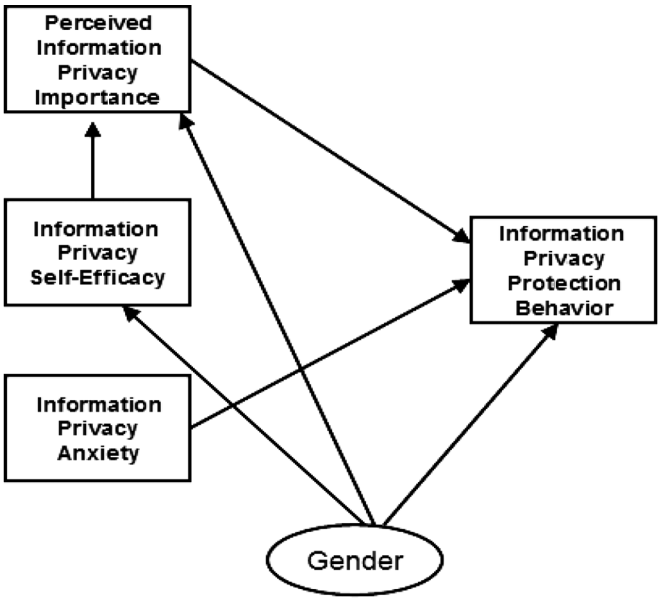

Fig. 1. Conceptual model.

According to Rogers, an individual's intention to protect him or herself depends on four factors: (1) the perceived severity of a threatening event; (2) the perceived probability of the occurrence; (3) the efficacy of the recommended preventive behavior that an individual expects to carry out; and (4) the individual's perceived self-efficacy (i.e., confidence in his or her ability to undertake the recommended preventive behavior) [14]. Protection Motivation Theory explains an individual's protection motivation as a result of threat assessment and coping appraisal. In this relationship, fear appeal plays a critical role in motivating a person's protection behavior [17], [18].

Based on Social Cognitive Theory and Protection Motivation Theory, this research presents a conceptual model, which is presented in Fig. 1.

Research Model and Hypotheses

Perceived Information Privacy Importance (PIPI) and Information Privacy Protection Behavior (IPPB) As one of the factors motivating an individual to perform a behavior, such as an academic task, perceived importance has been discussed in numerous studies. "Perceived importance" is defined as the degree to which an individual perceives a certain event or behavior to be important [19]–[21]. For example, Robin, Reidenbach, and Forrest measured the impact of perceived importance of ethics on the decision-making behavior of marketing personnel. They measured perceived importance (e.g., How important are business ethics for you?) by using a 9-point Likert scale [19]. Pajares and Graham investigated the role of perceived importance of mathematics with regard to math outcomes (i.e., math test results) [22].

In evaluating training programs, the employees' perceived importance of the training program plays an important role in increasing their motivation to join and do well in the training program [23]. The value, or importance of the object or activity, has a positive relationship with individual motivation [24]. Robin et al.'s research explored the impact of perceived importance of ethical issues on the decision-making and behavioral intentions of business mangers [19]. In the IT domain, ethical behavior in IT was also influenced by the user's perceived importance of IT ethics [25].

In this research, we propose a relationship between internet users' perceived importance of information privacy and their behavior to protect their privacy on the web. According to previous research results, which indicate a positive relationship between perceived importance in a certain domain and behavioral motivation to perform the activities related to that domain, we assume that internet users who place a higher value on the importance of information privacy will demonstrate more of a tendency to show online privacy protection behavior than the users who place a lower value on the importance of information privacy on the internet. Based on the discussion before, we propose Hypothesis 1:

> **H1**. Perceived information privacy importance will positively affect information privacy protection behavior.

Information Privacy Self-Efficacy (IPS) In Social Cognitive Theory [26], [27], self-efficacy is considered to be an important factor driving individuals' behavior [28], [29]. Individuals' self-efficacy beliefs operate on personal behavior through motivational, cognitive, and affective intervening processes [26]. Bandura et al. investigated the role of academic self-efficacy on academic performance and found a positive relationship between students' academic self-efficacy and their performance [29].

In the context of IT, the research suggests that individuals who possess high self-efficacy toward IT use IT more frequently [15], [16]. The research of Brown and Venkatesh also confirms that individuals' self-efficacy is a critical factor in

technology adoption [30]. People who have a higher level of self-efficacy toward a specific subject are more likely to confer a greater value to that subject. Wisenbaker, Scott, and Nasser show that students' strong cognitive competency toward statistics related to the greater value they placed on statistics [31]. Students' task-specific beliefs regarding their ability influence their values regarding a subject [32]. For example, students who believe they can do well at math tend to value mathematics more than children who do not believe in their math competency. Previous research also shows that students are much more likely to value math, language, art, and sports when they feel competent in a domain [33].

In the current study, we define information privacy self-efficacy as an individual's judgment of his or her capabilities to perform information privacy behavior. In other words, information privacy self-efficacy is about how confident children are in their skills and performing behaviors to protect their online privacy. Based on previous studies regarding self-efficacy, we propose that if students have high self-efficacy toward information privacy behavior, such as keeping personal information private during internet use, they will have a strong motivation to implement behavior that shows sensitivity to information privacy. Furthermore, students are more likely to value information privacy when they have a high level of self-efficacy in the information-security domain. Here, we propose the two-part hypothesis as follows.

H2a. Information privacy self-efficacy will positively affect perceived information privacy importance.

H2b. Information privacy self-efficacy will positively affect information privacy protection behavior.

The effect of education or informative programs is discussed as one of the important factors that influence an individual's self-efficacy and behavior. Strecher et al. find that self-efficacy plays a role in people's behavior in trying to improve their health conditions. According to their research, individuals' behaviors, such as cigarette smoking, weight control, and contraception, are positively related to their level of self-efficacy; in addition, they found that self-efficacy can be enhanced by educational programs [34]. Rubin et al. also found out that basic knowledge about diabetes and knowledge of ways to manage diabetes positively affect an individual's self-efficacy in coping with the disease [35]. Based on an experiment with 321 university students, Cody et al. found that enhanced knowledge about skin cancer strongly affected students' intention to protect their skin. Students who watched a video that provided knowledge about skin cancer had a higher intention to protect their skin than the group of students who watched a video that used emotional appeals about protecting skin [36]. In a study of privacy and email usage, Weisband and Reining found that education or training experiences influence users' privacy awareness [37].

Based on previous research findings, we assume that teens who have more opportunities to learn about information privacy at school and from parents and friends will have stronger self-efficacy in information privacy. Furthermore, if students are exposed to information privacy, they tend to have a strong, perceived importance of information privacy. In other words, if students hear about information security issues, such as how to protect privacy on the internet or avoid risks from computer viruses and spyware, they will develop a better perception of information privacy on the internet. Based on these assumptions, the two-part hypothesis about information privacy exposure is as follows.

H3a. Information privacy exposure will positively affect perceived information privacy importance.

H3b. Information privacy exposure will positively affect information privacy self-efficacy.

Information Privacy Anxiety (IPA) According to Protection Motivation Theory, the likelihood of engaging in protective behavior, such as risk avoidance, is positively related to factors, such as a high magnitude of danger, great probability of occurrence, existing effective actions to control consequences, and the capability to manage consequences. Among these factors, fear influences an individual's attitude and behavioral intention, which determine an individual's protective behavior [14], [17], [18], [38]. Research using Protection Motivation Theory as a framework suggests that fear is an effective mediator in people's intention to carry out protective behavior to avoid risks [39], [40]. In our study, we investigated the role of information privacy anxiety. Information privacy anxiety comes from an individual's cognitive assessment of his or her vulnerability and the possibility that an information privacy breach might occur. The previous Protection Motivation Theory literature leads us to argue that an individual's level of anxiety toward an online privacy breach will cause greater protective behavior as follows.

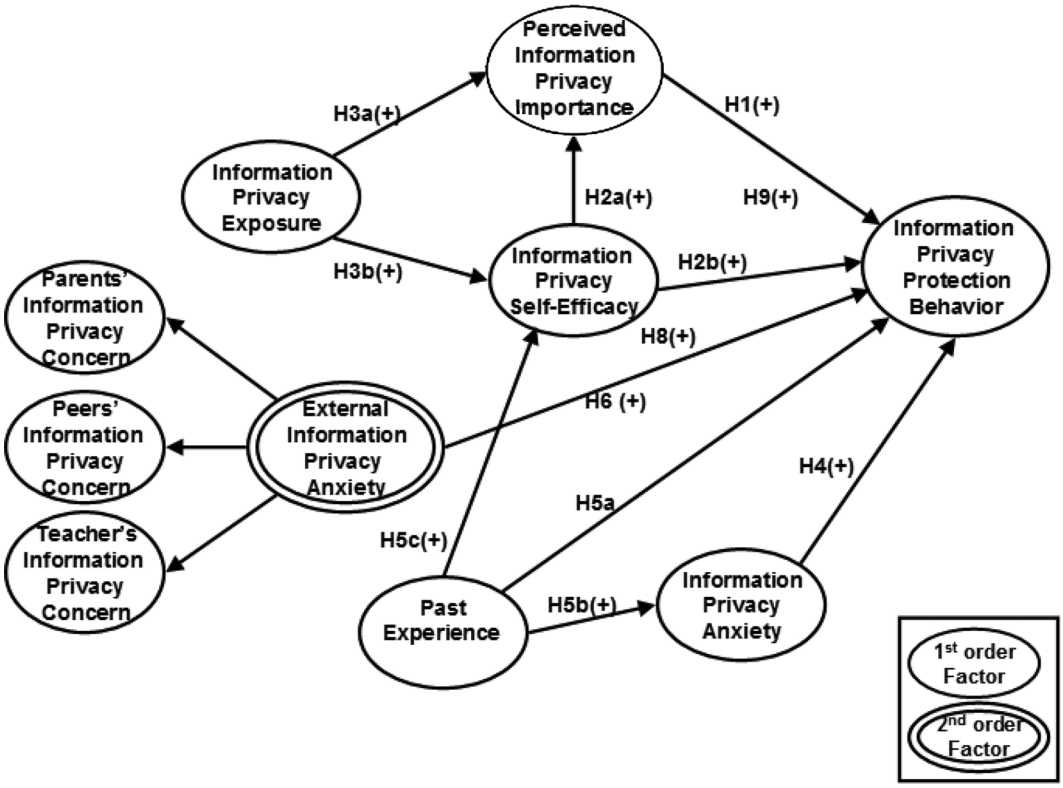

Fig. 2. Research model and hypothesis.

H4. Information privacy anxiety will positively affect information privacy protection behavior.

An individual's past experience regarding a domain also affects that person's decision making on behavior [41]. Cody et al.'s research indicates the impact of previous experience on health protection behavior. Their findings show that an individual who has a skin cancer experience has a stronger intention to protect skin and more of a tendency to exhibit protective behavior [36].

In this research, we discuss the impact of past experience on information privacy breaches. In our research, past bad experience (PE) with information privacy is represented by internet users' past experience with computer-virus hits, computer/information security problems, breaches of privacy, and bullying on the net. To investigate the role of bad experiences in the users' past, we hypothesize the following relationships between students' bad experiences and their self-efficacy, anxiety, and protective behavior toward online privacy incidents.

H5a. Past bad experience will have an impact on information privacy protection behavior.

H5b. Past bad experience will positively affect information privacy anxiety.

H5c. Past bad experience will negatively affect information privacy self-efficacy.

The influences of parents, teachers, and peers on adolescent behavior are extensively studied [42]–[45]. Carr and Weigand empirically tested the relationship between the students' physical education and the involvement of parents, teachers, and peers. They found that goal orientation toward physical education of students was positively influenced by a supportive climate of physical education [43]. Davies and Kandel found that the parental influence on adolescents' educational aspirations was stronger than peer influence. They also found that parental influence did not decline over the adolescent years [42].

Our research suggests a relationship between anxiety of parent, peer, and teacher and IPPB. We call the privacy concerns of parents, teachers, and peers external information privacy anxiety (EIPA). Based on the Protection Motivation Theory and prior research regarding the influence of parents, teachers, and peers, we assume a positive relationship between external information privacy anxiety and information privacy protection behavior.

H6. External information privacy anxiety will positively affect information privacy protection behavior.

Gender Several studies examine gender differences in technology adoption, usage behavior, and perception. These studies suggest that gender difference is a strong predicator of users' usage behavior and perception of technology. According to Kekelis et al., in the US, girls are given less computer-related support by their parents than boys [46]. Boys are encouraged to participate in hands-on experimenting more than girls, which gives boys the advantages of more confidence with technology and greater willingness to use it [47]. Gefen and Straub found that women and men differ in their perceptions and use of email [48]. Their study confirms that women and men differ in their perceptions of social presence via email and that women perceive email as more useful than men do. However, their study found that females perceive email to be more difficult to use than males do. Their research supports the notion that men feel more at ease with computers compared with women. Other studies point out that gender difference plays a significant role in online purchase intentions [49]–[51]. Also, one study showed that male employees in an organization had a tendency to use the internet more frequently than the female employees [52].

In the context of information privacy, women perceive online transactions to have greater risk than men do [53], and women have more concerns about information privacy [54]. Eccles et al. tested the effect of gender on the level of competency belief (i.e., self-efficacy) on various class activities, including math, reading, and sports [55]. Their results confirm that students' self-efficacy beliefs about various tasks vary by gender. Within the Protection Motivation Theory literature, it was found that women had greater knowledge and stronger intentions to prevent skin cancer than men did, but reported fewer high-risk behaviors [36].

Based on the aforementioned discussion, we argue that gender difference will have an impact on an individual's information privacy protection behavior, information privacy self-efficacy, and perceived information privacy importance:

H7. Information privacy protection behavior will vary by gender.

H8. Information privacy self-efficacy will vary by gender.

H9. Perceived information privacy importance will vary by gender.

TABLE I
RESEARCH HYPOTHESES

H#	Hypothesis
H1.	Perceived information privacy importance (PIPI) will positively affect information privacy protection behavior (IPPB).
H2a.	Information privacy self-efficacy (IPS) will positively affect perceived information privacy importance (PIPI).
H2b.	Information privacy self-efficacy (IPS) will positively affect information privacy protection behavior (IPPB).
H3a.	Information privacy exposure (IPE) will positively affect perceived information privacy importance (PIPI).
H3b.	Information privacy exposure (IPE) will positively affect information privacy self-efficacy (IPS).
H4.	Information privacy anxiety (IPA) will positively affect information privacy protection behavior (IPPB).
H5a.	Past bad experience (PE) will have an impact on information privacy protection behavior (IPPB).
H5b.	Past bad experience (PE) will positively affect information privacy anxiety (IPA).
H5c.	Past bad experience (PE) will negatively affect information privacy self-efficacy (IPS).
H6.	External information privacy anxiety (EIPA) will positively affect information privacy protection behavior (IPPB).
H7.	Information privacy protection behavior (IPPB) will vary by gender.
H8.	Information privacy self-efficacy (IPS) will vary by gender.
H9.	Perceived information privacy importance (PIPI) will vary by gender.

Fig. 2 presents our research model, and Table I lists our hypotheses.

RESEARCH DESIGN AND METHODOLOGY

We used a structured questionnaire survey. We surveyed school-age internet users who were middle school students. The survey was conducted at technology camps held in Maryland in June 2006 and in New York in February 2007. Out of 400 students, 285 responded to our survey, resulting in a 71.3% response rate. The average age was 13.6 years. Of the respondents, 45% were male, and 55% were female.

We used partial least square (PLS) to investigate the effect of the structural model. PLS enables the specification of the relationships among the constructs and the measures underlying each construct [56]. PLS, a variance-based approach, was first introduced by Wold. It focuses on maximizing the variance of the dependent variables explained by the independent variables instead of

TABLE II
CONSTRUCT DEFINITIONS

Construct	Definition
Information Privacy Protection Behavior (IPPB)	Users' behavior to protect their privacy on the internet, such as not giving out personal information (like home/email address, telephone number, school name) to unknown website, never opening email from unknown senders, and never having an online chat with a person whom they first met on the internet
Information Privacy Self-Efficacy (IPS)	Individuals' judgment of their capabilities to perform information privacy behavior
Perceived Information Privacy Importance (PIPI)	Individuals' perceived value of information privacy protection behavior
Information Privacy Exposure (IPE)	Experience of learning and hearing about information privacy in using internet and computer
Information Privacy Anxiety (IPA)	Individuals' concern and anxiety regarding expected occurrence of online privacy breach
Past Bad Experience (PE)	Individuals' personal experience of personal information breaches or threatening safety on the internet
External Information Privacy Anxiety (EIPA)	Individuals' beliefs coming from approval or disapproval of reference groups (e.g., parents, peers, and teachers) on information privacy protection behavior.

TABLE III
RELIABILITY VALUES FOR MEASUREMENT CONSTRUCT

	Construct	Number of Item	Cronbach's Alpha
1	Information Privacy Protection Behavior (IPPB)	4	0.710
2	Information Privacy Self-Efficacy (IPS)	3	0.766
3	Perceived Information Privacy Importance (PIPI)	3	0.944
4	Information Privacy Anxiety (IPA)	2	0.860
5	Parents' Information Privacy Concern (PIPC)	2	0.840
6	Peers' Information Privacy Concern (PEIPC)	2	0.820
7	Teacher's Information Privacy Concern (TIPC)	2	0.799

reproducing the empirical covariance matrix [57]. A covariance-based approach, such as LISREL or AMOS, is based on the assumption of a standard distribution of the data, and this also requires a large sample size. However, if the distribution is skewed or the sample size is not sufficient, a covariance-based approach can yield nonunique or otherwise improper solutions in some cases [58], [59]. In contrast, PLS has an advantage in that it involves no assumption about the population or scale of measurement and, consequently, it works without distributional assumptions and with nominal-, ordinal-, and interval-scaled variables [60].

PLS was an appropriate method for us compared with LISREL or AMOS for the following reasons. First, our data were highly skewed in information privacy protection behavior and information privacy exposure because they were collected from a summer technology camp of middle school students. Second, our study was exploratory, investigating a new area: information privacy.

We adopted many measurement indicators from prior literature and modified them to fit in the context of online information privacy. We adopted measurement indicators of IPS from Hackman and Oldham [61] and Hackman and Porter [62]. We used measures validated in previous research to control for measurement errors. However, we did construct some measures to reflect the context of information privacy. Since our study was the first study to explore preteen and early teens' behavior regarding information privacy protection behavior, we constructed our measurements (dependent variables IPPB1, IPPB2, IPPB3, IPPB4) based on research focusing on human behavior in relation to IT [63]–[65]. We adapted self-efficacy measures from relevant literature in educational psychology [29], [66]. We borrowed measures of perceived importance from Robin et al. [19], Pajares and Graham [22], and Eccles et al. [55], and adapted them to reflect the online privacy context.

We adopted measurement indicators for information privacy anxiety, past experience, and external influence from prior research that used Protection Motivation Theory. We modified the measures for the context of information privacy. We also constructed new measures for this study. Since our research participants were middle school students, we adjusted the level of difficulty and complexity of the survey questionnaire after we pilot tested it. The construct definitions are shown in Table II.

TABLE IV
INDIVIDUAL ITEM LOADING (PLS FACTOR LOADING)

Individual Item	Loading
Information Privacy Protection Behavior (IPPB) 1: Do not open email from unknown sender.	0.776
Information Privacy Protection Behavior (IPPB) 2: Do not download unknown files from known people and websites on the internet.	0.789
Information Privacy Protection Behavior (IPPB) 3: Do not give personal information (like home/email address, telephone number, school name) to unknown websites.	0.718
Information Privacy Protection Behavior (IPPB) 4: Do not give my personal information to people I first met on the internet.	0.710
Information Privacy Self-Efficacy (IPS) 1: Self-efficacy regarding internet privacy.	0.775
Information Privacy Self-Efficacy (IPS) 2: Self-efficacy regarding distinguishing between a trusted website and an unsafe website.	0.767
Information Privacy Self-Efficacy (IPS) 3: Self-efficacy regarding awareness of information security problems (e.g., virus, privacy breach, bullying on the net).	0.689
Perceived Information Privacy Importance (PIPI) 1: Perceived importance regarding personal information.	0.786
Perceived Information Privacy Importance (PIPI) 2: Perceived importance regarding protecting computer from computer viruses.	0.689
Perceived Information Privacy Importance (PIPI) 3: Perceived importance regarding internet privacy.	0.863
Information Privacy Anxiety (IPA) 1: Anxiety toward becoming a target of bullying on internet.	0.902
Information Privacy Anxiety (IPA) 2: Anxiety toward computer and privacy incidents.	0.838
Parents' Information Privacy Concern (PIPC) 1: Parents' concerns regarding internet safety.	0.929
Parents' Information Privacy Concern (PIPC) 2: Parents' concern regarding internet safety.	0.925
Peers' Information Privacy Concern (PEIPC) 1: Peers' awareness regarding internet privacy and safety.	0.927
Peers' Information Privacy Concern (PEIPC) 2: Peers' awareness regarding internet privacy and safety.	0.892
Teacher's Information Privacy Concern (TIPC) 1: Teacher's concerns regarding internet safety.	0.919
Teacher's Information Privacy Concern (TIPC) 2: Teacher's concerns regarding internet safety.	0.917

TABLE V
CROSS LOADINGS FOR THE MEASUREMENT MODEL

Individual Item	IPPB	PIPI	IPS	PIPC	PEIPC	TIPC	IPA
IPPB1	0.77	0.29	0.26	0.17	0.20	0.06	0.00
IPPB2	0.79	0.33	0.28	0.26	0.29	0.06	0.06
IPPB3	0.72	0.27	0.31	0.25	0.12	0.00	-0.03
IPPB4	0.71	0.28	0.28	0.15	0.11	-0.01	-0.02
PIPI1	0.34	0.79	0.34	0.27	0.17	-0.03	-0.07
PIPI2	0.20	0.69	0.40	0.20	0.11	0.00	0.00
PIPI3	0.39	0.86	0.35	0.30	0.21	0.05	0.03
IPS1	0.35	0.43	0.78	0.20	0.05	-0.05	-0.10
IPS2	0.24	0.29	0.77	0.13	0.12	0.10	-0.02
IPS3	0.21	0.29	0.69	0.10	0.16	0.12	-0.03
PIPC1	0.24	0.27	0.20	0.93	0.25	0.19	0.12
PIPC2	0.26	0.32	0.21	0.93	0.26	0.13	0.05
PEIPC1	0.25	0.18	0.15	0.26	0.92	0.12	0.14
PEIPC2	0.18	0.14	0.11	0.25	0.92	0.07	0.12
TIPC1	0.09	0.04	0.08	0.27	0.23	0.93	0.21
TIPC2	-0.06	-0.07	-0.07	0.20	0.10	0.90	0.25
IPA1	-0.03	-0.09	-0.11	0.10	0.20	0.19	0.90
IPA2	-0.06	-0.07	-0.06	0.05	0.03	0.06	0.84

To assess the reliability of measurement indicators, we employed Cronbach's alpha. We analyzed discriminant validity by comparing the average variance extracted (AVE) to the R^2 among the latent variables [67]. We carried out a factorial validity test of the measurement indicators with SPSS 12's exploratory factor analysis. To investigate the effect of gender on IPPB, the belief regarding self-efficacy, and importance of online information privacy, we used an independent sample t-test to compare males and females. We evaluated the effect of the structural model with a bootstrap resampling procedure within PLS by using 200 resamples.

As mentioned earlier, we investigated Cronbach's alpha to verify the internal consistency of each construct. Table III shows that the reliability test turned out to be reliable and that there was no significant defect in internal consistency.

To examine the validity of the measurement model, we carried out a composite reliability test and investigated the PLS factor loading and AVE.

As shown in Table IV, most of the standardized loadings of individual items were above the ideal cutoff level of 0.7 [68], [69]. However, the study of Hair et al. suggests a measurement item loads highly if its loading coefficient is above 0.60 and does not load highly if the coefficient is below 0.40. Only two out of the 18 reflective indicators had loadings lower than 0.70 (0.689), but they were higher or the same as the acceptable level of 0.60 [70]. It is important to point out that the value 0.689 is acceptable because our study is exploratory [70]. (The measurement items are shown in Table X.)

TABLE VI
CORRELATIONS AND AVE

Latent Variable		1	2	3	4	5	6	7	CR
1	IPPB	(0.749)							0.836
2	IPS	0.373	(0.745)						0.788
3	PIPI	0.396	0.462	(0.782)					0.825
4	IPA	-0.049	-0.103	-0.088	(0.757)				0.862
5	PIPC	0.263	0.166	0.244	0.216	(0.926)			0.924
6	PEIPC	0.024	0.012	-0.013	0.086	0.264	(0.909)		0.906
7	TIPC	0.234	0.146	0.173	0.145	0.190	0.185	(0.918)	0.915

Note: The number in the parentheses is the square root of AVE.

We also investigated cross-loadings of each item to compare each of them to all of the latent variables. Table V shows principal component analysis results from SPSS 12. We used Varimax with the Kaiser normalization rotation method.

We also carried out a composite reliability test. Values greater than 0.70 indicate acceptable values [71].

We tested discriminant validity by comparing AVE and the R^2 among the latent variables [67]. The AVE is calculated as $(\sum \lambda i^2)/((\sum \lambda i^2)) + (\sum (1 - \lambda i^2))$, where λ_i is the loading of each measurement item on its corresponding construct.

This comparison indicates that more variability is within a latent variable and its indicators than between the latent variables themselves. The results of the correlation matrix are shown in Table VI. All AVEs for the latent variables measured by reflective indicators were greater than the required minimum level of 0.50, and every construct had a larger square root of AVE than its correlations with other constructs. This result shows that our measurement model ensures discriminant validity [72]. The values of AVE, composite reliability, and correlation are presented in Table VI.

In our research model, there is a second-order factor (i.e., external influence). As shown in Fig. 2, the three dimensions of external influence are arranged in a second-order factor model, which depicts the multiple external influence dimensions as multidimensional entities of the higher second-order factor. All of its indicators had factor loadings above 0.70 and were significant at the 0.01 level. All indicators loaded higher on the first-order factors than on the second-order factors, and AVE of external influence was greater than the square of the correlations between it and its three first-order factors. This confirms that parents' information privacy concern, peers' information privacy concern, and a teacher's information privacy concern reflect the second-order factor well [73]. Regarding the relative importance of the three dimensions, the parents' information privacy concern is relatively more important than the peers' information privacy concern and a teacher's information privacy concern since their path coefficients from the external influence to parents' information privacy concern, peers' information privacy concern, and a teacher's information privacy concern were 0.771, 0.639, and 0.695, respectively. The correlations between second-order factors and other latent variables are shown in Table VII. A summary of results is presented in Table VIII.

RESULTS

Overall, the tests showed significant support for our model, and the amount of variance in the dependent latent variables explained by the model was moderate. Our research results are presented in Fig. 3 and Table VII. As shown in Fig. 3, most hypotheses are supported by data test results except for the hypothesis regarding the effect of IPA to IPPB and information privacy exposure (IPE) to PIPI. Around 24% of variance of the students' IPPB is explained by information privacy self-efficacy (IPS), PIPI, bad past experience (PE), and external information privacy anxiety (EIPA).

For H1, there was a significant and positive relationship between PIPI and IPPB ($\text{path} = 0.247$; $p < 0.005$). For H2a, IPS had a positive relationship with IPPB ($\text{path} = 0.207$; $p < 0.005$). H2b is also supported by data test results. Students' IPS had

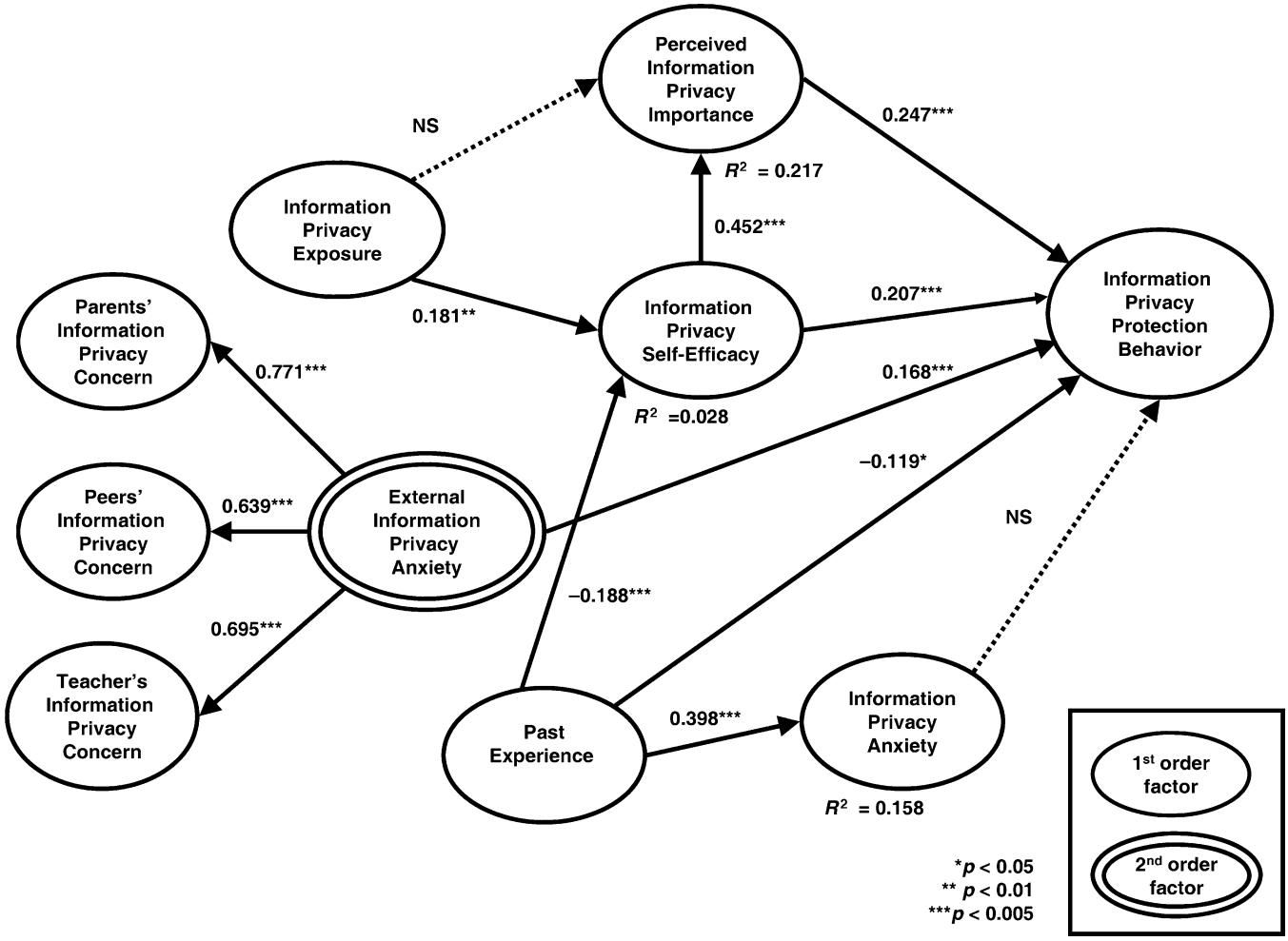

Fig. 3. Data-analysis results.

TABLE VII
CORRELATIONS BETWEEN SECOND-ORDER FACTORS AND OTHER LATENT VARIABLES

Latent Variable		1	2	3	4	5
1	IPPB	(0.749)				
2	IPS	0.373	(0.745)			
3	PIPI	0.396	0.462	(0.782)		
4	IPA	-0.049	-0.103	-0.088	(0.757)	
5	EIPA	0.263	0.166	0.244	0.216	(0.708)

Note: The number in the parentheses is the square root of AVE.

a strong positive effect on their PIPI (path $= 0.452$; $p < 0.005$). Our data results supported H3a, which postulated that an individual's IPE has a positive impact on IPS (path $= 0.181$; $p < 0.01$). In H4 and H6, which represent an individual's cognitive procedure regarding fear appeals, we found out that only EIPA has an impact on IPPB (path $= 0.168$; $p < 0.001$). H5a, 5b, and 5c were all supported by the results (5a, path $= -0.119$, $p < 0.5$; 5b, path $= 0.398$, $p < 0.001$; 5c, path $= -0.188$, $p < 0.001$). From these research findings, we realized that past experience of an online privacy breach can negatively affect users' IPPB and their self-efficacy of coping behavior. This finding indicates that students who experience an internet privacy breach or a computer security problem show less protection behavior on the internet, so they can be victims again in the future.

H7, H8, and H9 are related to gender differences in an individual's belief and behavior in online information privacy areas. Before we examined t-test results, we carried out Levene's test to investigate the equality of variance between the male and female groups. Levene's test (an F-test) tests that all variances are equal against the alternative hypothesis that the standard deviations are not all equal [74]. When the F resulting from Levene's test was significant at the 0.05 level, we used Welch modification to carry out t-tests. Each

TABLE VIII
GENDER DIFFERENCES IN INFORMATION PRIVACY PROTECTION BEHAVIOR AND BELIEF IN INFORMATION PRIVACY

	Girls			Boys			Levene's Test		Mean Difference		
Latent variable	*N*	*M*	*SD*	*N*	*M*	*SD*	*F*	*p*-value	*t*	*df*	*p*-value
IPPB	153	5.717	1.284	130	5.259	1.567	7.317	0.007**	-2.608	281.000	0.007**
IPS	153	5.762	1.009	129	5.734	1.091	0.198	0.657	-0.228	263.744	0.820
PIPI	154	6.470	0.743	130	6.308	0.867	4.791	0.031*	-1.695	282.000	0.091

*$p < 0.05$; **$p < 0.01$

TABLE IX
SUMMARY OF HYPOTHESES AND RESULTS

H#	Hypothesis	Results
H1.	Perceived information privacy importance will positively affect information privacy protection behavior.	Supported
H2a.	Information privacy self-efficacy will positively affect perceived information privacy importance.	Supported
H2b.	Information privacy self-efficacy will positively affect information privacy protection behavior.	Supported
H3a.	Information privacy exposure will positively affect perceived information privacy importance.	*Not Supported*
H3b.	Information privacy exposure will positively affect information privacy self-efficacy.	Supported
H4.	Information privacy anxiety will positively affect information privacy protection behavior.	*Not Supported*
H5a.	Past bad experience will have influence on information privacy protection behavior.	Supported
H5b.	Past bad experience will positively affect information privacy anxiety.	Supported
H5c.	Past bad experience will negatively affect information privacy self-efficacy.	Supported
H6.	External influence will positively affect information privacy protection behavior.	Supported
H7.	Information privacy protection behavior will vary by gender.	Supported
H8.	Information privacy self-efficacy will vary by gender.	*Not Supported*
H9.	Perceived information privacy importance will vary by gender.	Supported

group shows an unequal variance regarding one construct, IPPB ($p < 0.01$), so we used a modified procedure (the Welch modification) to compare the mean difference of the two groups. As shown in Table VIII, males and females show differences in their IPPB and PIPI. Thus, H7 is supported by data test results ($p < 0.01$), and H8 is also supported by data ($p < 0.5$). From the data-analysis results, we observe that female students are more likely to apply IPPB than male students as they value PIPI more. Interestingly, their belief about the self-efficacy level of online information privacy was not as different from the male group's.

DISCUSSION AND CONCLUSION

This study focuses on Social Cognitive Theory and Protection Motivation Theory to investigate the information protection behavior of internet users. In this study, we explored private-information-sharing behavior of preteen and early teen internet users because they are some of the most active users but also the most vulnerable in relation to online information privacy.

According to a survey of the US Department of Justice, one in five youths who regularly uses the internet received sexual solicitations or approaches during a one-year period, and 25% of youths surveyed received a sexual approach or solicitation over the internet in the past year [75]. More important, potential offenders and strangers have found that preteens and early teens are trusting, naïve, curious, and eager for attention and affection, making them easy targets for criminal acts. Since the internet provides anonymity to predators, the danger for children and teenagers increases, making them the most vulnerable group for information privacy [12].

We investigated the factors affecting middle school students' information protection behavior because they constitute a highly vulnerable group in terms of online privacy compared with adult internet

TABLE X
MEASUREMENT ITEMS

Individual Item	Measurement
IPPB1	I never open emails from unknown senders.
IPPB2	I never download files (like music, picture, game, movies, etc.) from the internet if the files are from unknown people.
IPPB3	I never give my personal information (like home/email address, telephone number, school name, etc.) to unknown websites.
IPPB4	I never give my personal information to people I first met on the internet.
IPS1	How good are you at keeping personal information (like name, photo, email, address, telephone number, etc.) secret from other internet users you don't trust?
IPS2	How good are you at noticing which web sites are not safe for children?
IPS3	How much are you aware of various computer/information security problems (like virus, privacy breach, bullying on the net, etc.)?
PIPI1	How important is it to keep your personal information (like address, telephone number, etc.) safe while using a computer?
PIPI2	How important is it to protect computers you use from viruses?
PIPI3	How important is it to protect your privacy (like giving your name, email, address, telephone number, etc.) on the internet?
EIPA1	My parents are very worried about bad people on the internet.
EIPA2	My parents are very worried about my safety on the internet.
EIPA3	My teachers are very worried about bad people on the Internet.
EIPA4	My teachers are very worried about students' safety on the internet.
EIPA5	My friends often talk about bad people on the internet.
EIPA6	My friends often talk about bad things happening on the Internet.
IPE1	Have you ever heard how to protect your personal information and yourself from school, parents, friends, community courses, media, or others?
IPA1	I may become a target of bullying on the internet one day.
IPA2	I may have a bad experience on the internet one day.
PE1	I have suffered from a computer/information security problem (like a virus, privacy breach, bullying on the net, etc.) in the past.

users. Our research findings suggest that students who have strong self-efficacy toward information privacy on the internet and have been exposed to online information privacy from school, parents, and media are more likely to practice online information privacy behaviors, such as not opening email from unknown senders, protecting personal information, and not downloading files from unknown people or websites.

Another factor that affected information privacy behavior was online privacy concerns from parents, teachers, and peers. Among these groups, the most influential group was parents, indicating that the parents who express their concerns about online safety positively contribute to their children's privacy protection behavior. The role of perceived importance of information privacy was very critical to determine students' behavior in maintaining their online privacy. As a mediator between users' self-efficacy and their protective behavior, the perceived importance of online information privacy had a significant impact on students' decisions to employ information protection behavior.

While a user's self-efficacy, perceived importance of information privacy, and external information privacy anxiety increase an individual's behaviors to keep online privacy, past experience of online privacy breaches negatively correlated with an individual's self-efficacy and information privacy protection behavior. From this finding, we expect that an internet user who has had a bad experience regarding online privacy will have more of a chance to suffer an online privacy breach again because of low self-efficacy about online privacy incidents and coping behaviors and less likelihood of executing behavior to protect himself or herself on the internet.

In terms of the role of fear appeal, only online privacy anxiety from the external environment had an impact on a user's online privacy protection behavior, while the internal anxiety of students themselves did not play a significant role. In addition to factors affecting the students' protection behavior on the web, we explored the impact of gender difference on perception of information privacy. Furthermore, we investigated potential behavioral differences in privacy protection behavior. Our data analysis strongly indicates that girls have more of a tendency to practice protective behavior on the web. Our results also suggest that an online user's level of perception about information privacy importance can cause different privacy protection behavior. In addition, as shown in Table VIII, the mean of perceived information privacy importance for women is higher than that for men, so we can say that girls consider online privacy to be more important than boys do.

In light of our research results, we need to provide more information about how preteens and

early teens can protect themselves from online privacy incidents. More important, online privacy information and education opportunities that promote privacy protection behaviors are necessary.

The limitation of this study is the sample characteristic. First, we have investigated middle school students in two states: New York and Maryland. A more random sample may need to be used. Second, since our study is the first to explore internet users' online privacy protection behavior, and our sample is limited to preteens and early teens, some of the measurement indicators did not have a high loading value. To obtain solid measurement items for online privacy protection behavior, more research based on larger and varied samples needs to be carried out. For a subsequent study, a higher value will be expected. Third, even though our current study focuses on preteens and early teens, our research model can be expanded to adult internet users. We need to carry out further research that focuses on adult users as well.

Although our empirical research results are based on the data set of preteen and early teens' behavior regarding online information privacy, our research findings and the model can be applied to understanding general internet users' behavior in relation to private information sharing. Internet users who have more knowledge and self-efficacy regarding online privacy issues show more tendency to protect their personal information. However, our results suggest that users who suffered negative experiences (e.g., privacy breaches, information security/privacy incidents, or computer viruses) showed less protective behavior in sharing their personal information. We can interpret this finding to mean that internet users with a bad experience are more likely to become victims of privacy incidents in the future. In addition, external factors, educational opportunities regarding internet privacy, computer security, and concerns from parents, teachers, and peers also play a significant role in users' protective behaviors since their perceived value on the importance of online privacy and self-efficacy level directly affect the users' protective behavior. Another interesting finding is that female internet users think that their private information is more important than male internet users do and, thus, show more protective behavior.

We believe that our research framework and empirical results contribute to understanding users' behaviors toward online information privacy and protection of internet users from information privacy incidents.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation under Grant 0420448. The authors thank the IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION editors and referees for their critical comments that have greatly improved this paper. The usual disclaimer applies.

REFERENCES

[1] A. F. Westin, *Privacy and Freedom*. New York: Athenaeum, 1967.
[2] V. Perugini, "Anytime, anywhere: The social impact of emerging communication technology," *IEEE Trans. Prof. Commun.*, vol. 39, no. 1, pp. 4–16, Mar., 1996.
[3] P. A. Chociey, "'Who's reading my e-mail?': A study of professionals' e-mail usage and privacy perceptions in the workplace," *IEEE Trans. Prof. Commun.*, vol. 40, no. 1, pp. 34–41, Mar., 1997.
[4] US House of Representatives. 107th Session. (2001, May 8). Opinion Surveys: What Consumers Have to Say About Information Privacy. [Online]. Available: http://bulk.resource.org/gpo.gov/hearings/107h/72825.pdf
[5] E. M. Caudill and P. E. Murphy, "Consumer online privacy: Legal and ethical issues," *J. Public Policy Market.*, vol. 19, no. 1, pp. 7–19, 2000.
[6] Federal Trade Commission, Privacy initiatives. [Online]. Available: http://www.ftc.gov/privacy/
[7] National Telecommunications and Information Administration. (2002, Feb.). A nation online: How Americans are expanding their use of the internet. [Online]. Available: http://www.ntia.doc.gov/ntiahome/dn/nationonline_020502.htm
[8] X. Cai and W. Gantz, "Online privacy issues associated with web sites for children," *J. Broadcast. Electron. Media*, vol. 44, no. 2, pp. 197–214, 2000.
[9] S. Chai, J. Lee, and H. R. Rao, "Managing private information safety in blogs," presented at the 2nd Secure Knowledge Management Workshop, Brooklyn, NY, Sep. 28–29, 2006.
[10] J. Turow. (2003, Jun.). Americans and online privacy: The system is broken. Annenberg Public Policy Center, Univ. Pennsylvania. [Online]. Available: http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf
[11] J. Turow. (2001, Mar.). Privacy policies on children's websites: Do they play by the rules? Annenberg Public Policy Ctr., Univ. Pennsylvania. [Online]. Available: http://www.asc.upenn.edu/usr/jturow/PrivacyReport.pdf
[12] US Department of Justice. (2007, May 4). Children as targets of internet crimes–Who is vulnerable? *Internet Crimes Against Children.* [Online]. Available: http://www.ojp.usdoj.gov/ovc/publications/bulletins/internet_2_2001/internet_2_01_3.html
[13] A. Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory*. Upper Saddle River, NJ: Prentice-Hall, 1986.

[14] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *J. Psychol.*, vol. 91, no. 1, pp. 9–114, 1975.
[15] D. R. Compeau and C. A. Higgins, "Application of social cognitive theory to training for computer skills," *Inf. Syst. Res.*, vol. 6, no. 2, pp. 118–143, 1995.
[16] D. Compeau, C. A. Higgins, and S. Huff, "Social cognitive theory and individual reactions to computing technology: A longitudinal study," *MIS Quart.*, vol. 23, no. 2, pp. 145–158, 1999.
[17] M. Brouwers and R. M. Sorrentino, "Uncertainty orientation and protection motivation theory: The role of individual differences in health compliance," *J. Personality Soc. Psychol.*, vol. 65, no. 1, pp. 102–112, 1993.
[18] S. Wurtele and J. Maddux, "Relative contributions of protection motivation theory components in predicting exercise intentions and behavior," *Health Psychol.*, vol. 6, no. 5, pp. 453–466, 1987.
[19] D. P. Robin, R. E. Reidenbach, and P. J. Forrest, "The perceived importance of an ethical issue as an influence on the ethical decision-making of ad managers," *J. Bus. Res.*, vol. 35, no. 1, pp. 17–28, 1996.
[20] K. P. Grant, C. R. Baumgardner, and G. S. Shane, "The perceived importance of technical competence to project managers in the defense acquisition community," *IEEE Trans. Eng. Manage.*, vol. 44, no. 1, pp. 12–19, 1997.
[21] H. A. Hausenblas and A. V. Carron, "Group cohesion and self-handicapping in female and male athletes," *J. Sport Exercise Psychol.*, vol. 18, no. 2, pp. 132–143, 1996.
[22] F. Pajares and L. Graham, "Self-efficacy, motivation constructs, and mathematics performance of entering middle school students," *Contemp. Educ. Psychol.*, vol. 24, no. 2, pp. 124–139, 1999.
[23] W. C. Tsai and W. T. Tai, "Perceived importance as a mediator of the relationship between training assignment and training motivation," *Personnel Rev.*, vol. 32, no. 2, pp. 151–163, 2003.
[24] J. S. Eccles and A. Wigfield, "Motivational beliefs, values, and goals," *Annu. Rev. Psychol.*, vol. 53, no. 1, pp. 109–132, 2002.
[25] L. N. K. Leonard, T. P. Cronan, and J. Kreie, "What influences IT ethical behavior intentions-planned behavior, reasoned action, perceived importance, or individual characteristics?," *Inf. Manage.*, vol. 42, no. 1, pp. 143–158, 2004.
[26] A. Bandura, "Human agency in social cognitive theory," *Amer. Psychol.*, vol. 44, no. 9, pp. 1175–1184, 1989.
[27] A. Bandura, "Self-efficacy mechanism in human agency," *Amer. Psychol.*, vol. 37, no. 2, pp. 122–147, 1982.
[28] A. Bandura and D. Cervone, "Self-evaluative and self-efficacy mechanisms governing the motivational effects of goal systems," *J. Personal. Soc. Psychol.*, vol. 45, no. 5, pp. 1017–1028, 1983.
[29] A. Bandura, C. Barbaranelli, G. Caprara, and C. Pastorelli, "Multifaceted impact of self-efficacy beliefs on academic functioning," *Child Develop.*, vol. 67, no. 3, pp. 1206–1222, 1996.
[30] S. A. Brown and V. Venkatesh, "A model of adoption of technology in the household: A baseline model test and extension incorporating household life cycle," *MIS Quart.*, vol. 29, no. 3, pp. 399–426, 2005.
[31] J. Wisenbaker, J. Scott, and F. Nasser, "Structural equation models relating attitudes about and achievement in introductory statistics courses: A comparison of results from the U.S. and Israel," presented at the 9th Int. Congr. Mathematics Education, Tokyo, Japan, Jul. 31–Aug. 6, 2000.
[32] A. Wigfield and J. S. Eccles, "Expectancy-value theory of achievement motivation," *Contemp. Educ. Psychol.*, vol. 25, no. 1, pp. 68–81, 2000.
[33] J. E. Jacobs, S. Lanza, D. W. Osgood, J. S. Eccles, and A. Wigfield, "Changes in children's self-competence and values: Gender and domain differences across grades one through twelve," *Child Develop.*, vol. 73, no. 2, pp. 509–527, 2002.
[34] V. J. Strecher, B. M. DeVellis, M. H. Becker, and I. M. Rosenstock, "The role of self-efficacy in achieving health behavior change," *Health Educ. Behav.*, vol. 13, no. 1, pp. 73–92, 1986.
[35] R. R. Rubin, M. Peyrot, and C. D. Saudek, "The effect of a diabetes education program incorporating coping skills training on emotional well-being and diabetes self-efficacy," *Diabetes Educ.*, vol. 19, no. 3, pp. 210–216, 1993.
[36] R. Cody and C. Lee, "Behaviors, beliefs, and intentions in skin cancer prevention," *J. Behav. Med.*, vol. 13, no. 4, pp. 373–389, 1990.
[37] S. P. Weisband and B. A. Reinig, "Managing user perceptions of email privacy," *Commun. ACM*, vol. 38, no. 12, pp. 40–48, 1995.
[38] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social Psyhophysiology*, J. T. Cacioppo and R. E. Petty, Eds. New York: Guilford, 1983, pp. 153–174.
[39] J. F. Tanner, Jr., J. B. Hunt, and D. R. Eppright, "The protection motivation model: A normative model of fear appeals," *J. Market.*, vol. 55, no. 3, pp. 26–45, 1991.
[40] K. Witte, "The role of threat and efficacy in AIDS prevention," *Int. Quart. Community Health Educ.*, vol. 12, no. 3, pp. 225–249, 1992.
[41] S. F. Sonmez and A. R. Graefe, "Determining future travel behavior from past travel experience and perceptions of risk and safety," *J. Travel Res.*, vol. 37, no. 2, pp. 171–177, 1998.
[42] M. Davies and D. B. Kandel, "Parental and peer influences on adolescents' educational plans: Some further evidence," *Amer. J. Sociol.*, vol. 87, no. 2, pp. 363–387, 1981.
[43] S. Carr and D. A. Weigand, "Parental, peer, teacher and sporting hero influence on the goal orientations of children in physical education," *Eur. Phys. Educ. Rev.*, vol. 7, no. 3, pp. 305–328, 2001.
[44] H. Ma, D. Shek, P. Cheung, and C. O. Lam, "Parental, peer, and teacher influences on the social behavior of Hong Kong Chinese adolescents," *J. Gen. Psychol.*, vol. 161, no. 1, pp. 65–78, 2000.

[45] R. George and D. Kaplan, "A structural model of parent and teacher influences on science attitudes of eighth graders: Evidence from NELS: 88," *Sci. Educ.*, vol. 82, no. 1, pp. 93–109, 1998.
[46] L. S. Kekelis, R. W. Ancheta, and E. Heber, "Hurdles in the pipeline: Girls and technology careers," *Frontiers: J. Women Studies*, vol. 26, no. 1, 2005.
[47] J. Countryman, A. Feldman, L. Kekelis, and E. Spertus, "Developing a hardware and programming curriculum for middle school girls," *ACM SIGCSE Bull.*, vol. 34, no. 2, pp. 44–47, 2002.
[48] D. Gefen and D. W. Straub, "Gender differences in the perception and use of E-mail: An extension to the technology acceptance model," *MIS Quart.*, vol. 21, no. 4, pp. 389–400, 1997.
[49] E. Y. Kim and Y. K. Kim, "Predicting online purchase intentions for clothing products," *Eur. J. Market.*, vol. 38, no. 7, pp. 883–897, 2004.
[50] T. J. Larson and O. Sorebo, "Impact of personal innovativeness on the use of the internet among employees at work," *J. Organ. End User Comput.*, vol. 17, no. 2, pp. 43–63, 2005.
[51] C. V. Slyke, C. L. Comunale, and F. Belanger, "Gender differences in perceptions of Web-based shopping. Association for Computing Machinery," *Commun. ACM*, vol. 45, pp. 82–86, 2002.
[52] T. J. Larsen and O. Sorebo, "Impact of personal innovativeness on the use of the internet among employees at work," *J, Organ. End User Comput.*, vol. 17, no. 2, pp. 43–63, 2005.
[53] E. Garbarino and M. Strahilevitz, "Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation," *J. Bus. Res.*, vol. 57, no. 7, pp. 768–775, 2004.
[54] M. Phillip and R. Suri, "Impact of gender differences on the evaluation of promotional emails," *J. Advert. Res.*, vol. 44, no. 4, pp. 360–368, 2004.
[55] J. Eccles, A. Wigfield, R. D. Harold, and P. Blumenfeld, "Age and gender differences in children's self- and task perceptions during elementary school," *Child Develop.*, vol. 64, no. 3, pp. 830–847, 1993.
[56] H. Wold, "Introduction to the second generation of multivariate analysis," in *Theoretical Empiricism*, H. Wold, Ed. New York: Paragon House, 1989, pp. vii–xi.
[57] H. Wold, "Partial least squares," in *Encyclopedia of Statistical Sciences*, S. Kotz and N. L. Johnson, Eds. New York: Wiley, 1985, pp. 581–591.
[58] C. Fornell, *A Second Generation of Multivariate Analysis: Measurement and Evaluation.* New York: Praeger, 1982.
[59] C. Fornell and F. L. Bookstein, "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory," *J. Market. Res.*, vol. 19, no. 4, pp. 440–452, 1982.
[60] M. Haenlein and A. M. Kaplan, "A beginner's guide to partial least squares analysis," *Understand. Stat.*, vol. 3, no. 4, pp. 283–297, 2004.
[61] J. R. Hackman and G. R. Oldham, "Motivation through the design of work: Test of a theory," *Organ. Behav. Human Perform.*, vol. 16, pp. 250–279, 1976.
[62] J. R. Hackman and L. W. Porter, "Expectancy theory of predictions of work effectiveness," *Organ. Behav. Human Perform.*, vol. 3, pp. 417–426, 1968.
[63] C. E. Downing, "System usage behavior as a proxy for user satisfaction: An empirical investigation," *Inf. Manage.*, vol. 35, no. 4, pp. 203–216, 1999.
[64] V. Venkatesh and M. G. Morris, "Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior," *MIS Quart.*, vol. 24, no. 1, pp. 115–139, 2000.
[65] F. D. Davis, "User acceptance of information technology: System characteristics, user perceptions and behavioral impacts," *Int. J. Man-Machine Studies*, vol. 38, no. 3, pp. 475–487, 1993.
[66] N. Choi, D. R. Fuqua, and B. W. Griffin, "Exploratory analysis of the structure of scores from the multidimensional scales of perceived self-efficacy," *Educ. Psychol. Meas.*, vol. 61, no. 3, pp. 475–489, 2001.
[67] C. Fornell and D. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Market. Res.*, vol. 18, no. 1, pp. 39–50, 1981.
[68] W. W. Chin, "The partial least squares approach to structural equation modeling," in *Modern Methods for Business Research*, G. A. Marcoulides, Ed. Mahwah, NJ: Lawrence Erlbaum Associates, 1998, pp. 295–336.
[69] D. Barclay, C. Higgins, and R. Thompson, "The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration," *Technol. Studies*, vol. 2, no. 2, pp. 285–324, 1995.
[70] J. F. Hair, Jr., R. E. Anderson, R. L. Tatham, and W. Black, *Multivariate Data Analysis,* 5th ed. Upper Saddle River, NJ: Prentice-Hall, 1998.
[71] C. E. Werts, R. L. Linn, and K. G. Jöreskog, "Intraclass reliability estimates: Testing structural assumptions," *Educ. Psychol. Meas.*, vol. 34, no. 1, pp. 25–33, 1974.
[72] W. W. Chin, "Issues and opinion on structural equation modeling," *MIS Quart.*, vol. 22, no. 1, pp. 7–16, 1998.
[73] W. W. Chin and A. Gopal, "Adoption intention in GSS: Relative importance of beliefs," *ACM SIGMIS Database*, vol. 26, no. 2–3, pp. 42–64, 1995.
[74] M. B. Brown and A. B. Forsythe, "Robust tests for the equality of variances," *J. Amer. Statist. Assoc.*, vol. 69, no. 346, pp. 364–367, 1974.
[75] D. Finkelhor, K. J. Mitchell, and J. Wolak, "Highlights of the youth internet safety survey," Juvenile Justice Fact Sheet 200104, Washington DC, US Government Printing Office, pp. 1–2, 2001.

Sangmi Chai received the M.B.A. degree from Seoul National University, Seoul, Korea, and is currently pursuing the Ph.D. degree in Management Systems and Science at the State University of New York Buffalo. Her research interests include information security, human-computer interface, ethical issues and information privacy, information technology diffusion in the public sector, and cybersecurity.

Sharmistha Bagchi-Sen is Professor of Geography at the State University of New York (SUNY) Buffalo and is Director of Graduate Studies in the Department of Geography. She has been published in many articles on foreign direct investment in the export market of the US, development strategies by small and medium manufacturing firms, and employment patterns. She is an advisory committee member for the Baldy Center for Law and Social Policy, and she was a member of the steering and executive committees for the Institute for Research and Education on Women and Gender at SUNY Buffalo.

Claudia Morrell received the M.A. degree from Loyola College, Baltimore, MD and the M.S. degree from the University of Wisconsin-Madison. She is CEO of Multinational Development of Women in Technology, Baltimore.

H. R. Rao is Professor of Management Information Systems and Science at the State University of New York Buffalo. He has chaired sessions at international conferences, presented numerous papers, and received funding for his research from the National Science Foundation, the Department of Defense, and the Canadian Embassy. He is coeditor of *Information Systems Frontiers*.

Shambhu J. Upadhyaya (SM'01) is Associate Professor in the Computer Science and Engineering Department at the State University of New York Buffalo, where he directs the Center of Excellence in Information Systems Assurance Research and Education. He is an associate editor of the IEEE TRANSACTIONS ON COMPUTERS and a member of the editorial board of the *International Journal on Reliability, Quality, and Safety Engineering*.