Communications of the Association for Information Systems

Volume 28 Article 28

5-2011

Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework

Yuan Li
Division of Business, Mathematics and Sciences, Columbia College, Columbia, South Carolina, yli@columbiasc.edu

Recommended Citation

Li, Yuan (2011) "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems*: Vol. 28 , Article 28.
DOI: 10.17705/1CAIS.02828
Available at: https://aisel.aisnet.org/cais/vol28/iss1/28

Communications of the Association for Information Systems

CAIS

Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework

Yuan Li

Division of Business, Mathematics and Sciences, Columbia College, Columbia, South Carolina

yli@columbiasc.edu

Abstract:

In the e-commerce environment, individuals' concerns for online information privacy play critical roles in determining their intention to use the Internet to provide personal information for services and transactions. Understanding this relationship has important implications for e-commerce. Despite much research in this area, an overarching picture of the relationship between information privacy concerns and the antecedent and consequence factors is yet to be drawn. Based on a review on empirical studies in this area, this research summarizes the conceptualizations of privacy concerns and the antecedents and consequences. An integrative framework is developed to illustrate the relationships between the factors. In this framework, a person's concern for information privacy regarding a specific e-commerce website is distinguished from his/her concern for information privacy regarding the general e-commerce environment. These two forms of privacy concerns have distinct impacts on a person's online behavior. Their relationships with multiple antecedent and consequence factors are analyzed.

Keywords: Information privacy, concerns for information privacy (CFIP), General CFIP, Specific CFIP, trust belief, risk belief, literature review

Volume 28, Article 28, pp. 453-496, May 2011

The manuscript was received 7/21/2010 and was with the authors 4 months for 1 revision.

I. INTRODUCTION

With the development of e-commerce, individuals' information privacy, referring to the ability of individuals to personally control information about themselves [Smith et al., 1996], is becoming critically important to individuals, organizations, industries, governments, and the global community [Chan et al., 2005; Davison et al., 2003]. A recent article in *Businessweek* reported the concerns of the United States congress about social network giant Facebook.com's practices of sharing the private information of its users without their consent [MacMillan, 2010]. Similar concerns were expressed in other major media [e.g., Gross, 2010]. Although organizations, industries, and governments play important roles in protecting consumers' online information privacy [Wang et al., 1998] and consumers may take protective actions to reduce the risks [Chen and Rea, 2004; Son and Kim, 2008; Zviran, 2008], a full protection of privacy has not been achieved in the e-commerce environment. More studies are needed to understand online consumers' privacy concerns and the factors that influence the concerns.

Scholars from multiple disciplines, especially the Information Systems (IS) field, have conducted extensive research on individuals' online information privacy based on constructs such as perceived information privacy [e.g., Frye and Dornisch, 2010; Joinson et al., 2010; Shin, 2010] and information privacy concerns [e.g., Dinev and Hart, 2004, 2005, 2006; Smith et al., 1996]. The former is a direct measure of a person's perception of his/her information privacy on the Internet, and the latter captures the worries about privacy control. Although these are two opposing constructs, they share many antecedents and consequences with reverse relationships [e.g., Casalo et al., 2007; Eastlick et al., 2006] and have been used interchangeably across studies [e.g., Cases et al., 2010]. To develop a comprehensive view on online information privacy, this study considers both while emphasizing the privacy concern construct due to its popularity in research.

To gain deep insight into privacy concerns, scholars have conducted research to measure the construct [e.g., Malhotra et al., 2004; Smith et al., 1996; Stewart and Segars, 2002] and to analyze the associated factors [e.g., Angst and Agarwal, 2009; Culnan and Armstrong, 1999; Hann et al., 2007; Pavlou et al., 2007; Son and Kim, 2008; Van Slyke et al., 2006]. Although significant progress has been made in this area, there are several important issues to be addressed. First, as a large number of factors associated with privacy concerns were recognized, an integrative framework is needed to consolidate the factors and build a holistic view of privacy concerns. Although some preliminary frameworks were introduced in literature [e.g., Peltier et al., 2009; Xu et al., 2008], the scopes of the frameworks were restricted to a small number of factors. To expand knowledge in this area, it is necessary to incorporate additional factors in a more comprehensive view.

Related to the above issue is the poor organization of the factors associated with privacy concerns. Many different types of antecedents were recognized, ranging from personal characteristics to culture and regulatory structures [e.g., Bellman et al., 2004; Junglas et al., 2008], but from what perspective they affect privacy concerns is not well known. This raises the question of how to effectively apply the factors to protect individual privacy. Similarly, different consequences of privacy concerns were studied, including privacy attitudes, behavioral intentions, and actual behaviors [e.g., Son and Kim, 2008], but how these consequences are organized and interrelated is not systematically analyzed, either. Without a proper organization of the factors, it is difficult to use the factors to develop proper action plans to protect privacy.

The third issue deals with the lack of synthesis in this area. For example, the conceptualizations and measurements of the privacy concern construct differ significantly across studies [e.g., Buchanan et al., 2007; Malhotra et al., 2004; Smith et al., 1996]. No horizontal comparison of these measurements was attempted, so that the potential impact on further research is unknown. Another example is the impact of information on privacy: various types of information, such as medical records [Rohm and Milne, 2004], identifiable and non-identifiable information [Faja and Trimi, 2006] and exclusive information [Chen et al., 2009] were examined in studies, but a generalization across the information types was not proposed, raising the question of how to evaluate new types of information in further research. As studies in this area progress, a synthesis and consolidation is needed to clarify these critical concepts.

Finally, the literature presented controversial relationships between privacy concerns and some key constructs such as trust belief and risk belief. Some studies treated trust as a predictor of privacy [Pavlou et al., 2007; Tsarenko and Tojib, 2009], while others treated it as a consequence [Casalo et al., 2007; Chiu et al., 2009; Eastlick et al., 2006; Liu et al., 2005; Malhotra et al., 2004; Van Slyke et al., 2006]. Similarly, risk belief was studied as both the antecedent [Dinev et al., 2006; Dinev and Hart, 2006; Xu et al., 2008] and the consequence of privacy concerns [Cocosila et al., 2009; Malhotra et al., 2004; Van Slyke et al., 2006], calling for clarifications.

To address the above issues, this article follows the literature review study guidelines [Schwarz et al., 2007] to provide a review on information privacy research. Topics discussed include the measurement of privacy concerns, antecedents, consequences, and moderating effects. Based on the review, an integrative framework is developed to illustrate the relationships between the factors and to highlight opportunities for further improvement. The study attempts to achieve several objectives: (1) to integrate research in the area and develop a comprehensive view, (2) to organize the antecedent and consequence factors for a better understanding of their effects, (3) to synthesize research findings to clarify concepts, and (4) to provide solutions to some of the controversial relationships.

The rest of the article is organized as follows. First, the research method is described, followed by the report of the review findings. The integrative framework for further research is then developed, and the key relationships in the framework are proposed. Finally, implications, future research directions and limitations are discussed.

II. RESEARCH METHOD

This research follows the common approaches of literature review study [e.g., Lee et al., 2007; Saeed et al., 2003; Schwarz et al., 2007]. To perform a rigorous analysis of the content in each article, the content analysis method is used. Content analysis is a systematic, objective, and quantitative analysis of message characteristics [Neuendorf, 2002]—in this case the research articles. It provides a more scientific approach to examining literature than literary criticism [Kassarjian, 1977] and has been applied in literature review research [e.g., Brutus et al., 2010; Jourdan et al., 2008]. Specifically, the current study adopts the interpretative type of content analysis in order to develop a theoretical framework from the observations of existing literature in the area; to this end, conceptual categories are developed to enable comparative analysis [Neuendorf, 2002, p. 6].

Although Neundorf [2002] introduced a popular framework of content analysis consisting of nine steps, this research adopts a shorter framework by Kassarjian [1977]. First, the sample for study is selected from the available population of documents. This step consists of the specification of search criteria, the selection of journal pool, search string and time range, and the extraction of research articles from the pool. The second step is to determine the unit of analysis and coding scheme. In this review, constructs and effect sizes reported in each article are coded, along with descriptive information, such as research methods and sample sizes. The third step is to categorize the content according to predetermined rules. The last step analyzes the data. These steps are described in the next sections.

Inclusion and Exclusion Criteria

It goes beyond the scope of this research to review all the studies on information privacy; instead, this research examines empirical studies on individuals' online information privacy and its impact on their online behavior. A detailed list of inclusion and exclusion criteria is described in Table 1. First of all, this research reviews only studies in the e-commerce domain; other privacy issues such as workplace privacy [e.g., Allen et al., 2007] are not discussed. Although distinctions exist between e-commerce models such as e-tailing and social-networking, their boundaries are becoming less clear as e-commerce evolves, and consumers may exert similar activities on either site while holding similar concerns. For example, a person may join others on an e-tailing website to discuss product features, or click on an ad on a social-networking site to purchase products. In either case, the person's information may be collected or used without his/her knowledge, causing privacy concerns. While some studies have focused on certain types of websites such as social networking sites [e.g., Shin, 2010], others tended to move beyond the differences between e-commerce models and recognized similar antecedents and consequences of privacy concerns [e.g., Xu et al., 2008]. In order to provide a comprehensive review, privacy issues regarding all e-commerce models are summarized.

The second criterion deals with individual-level of study. Other levels of research such as organizational level [e.g., Greenaway and Chan, 2005; Schwaig et al., 2006] are not discussed. Third, this review examines empirically tested behavioral studies only, for the purpose of developing an integrative framework based on empirical evidences. This excludes other types of research such as mathematical modeling [e.g., Chellappa and Shivendu, 2007; Garfinkel et al., 2007; Li and Sarkar, 2006] and technology frameworks [e.g., Smyth, 2007]. Descriptive studies, although containing empirical evidences [e.g., Paine et al., 2007], are also excluded due to the lack of causality measures.

Additionally, only studies that contain a privacy or privacy concern related construct are included; studies that address privacy issues without a qualified construct are ignored [e.g., Aljukhadar et al., 2010; Hann et al., 2007]. In fact, many studies measure privacy beliefs through other surrogates such as trust beliefs or risk beliefs [e.g.,

Table 1: Literature Selection Criteria

Criteria	Inclusion criteria	Exclusion criteria (with examples)
Domain of research	Privacy in e-commerce (such as e-tailing, e-content, and social networking)	Privacy in workplace (e.g., Allen et al., 2007)
Level of research	Individual level	Other levels of study such as organizational level (e.g., Greenaway and Chan, 2005; Schwaig et al., 2006)
Types of research	Behavioral studies	Other types of studies such as mathematical and economic modeling (e.g., Chellappa and Shivendu, 2007; Garfinkel et al., 2007; Li and Sarkar, 2006), technology papers (e.g., Smyth, 2007), conceptual papers (e.g., Conger, 2009), and laws and public policy papers (e.g., Ciocchetti 2007; DeMarco, 2006)
Methods of research	Empirical studies (such as surveying and experimentation)	Qualitative research and case studies (e.g., Culnan and Williams, 2009) and descriptive studies (e.g., Paine et al., 2007)
Key constructs	Must contain perceived privacy or privacy concern related constructs	Studies without a qualified construct (e.g., Aljukhadar et al., 2010; Hann et al., 2007)
Sources of publications	Peer-reviewed academic journals and the proceedings of the International Conference on Information Systems	Professional journals (e.g., Brown, 2009)

Aljukhadar et al., 2010]. Nevertheless, trust and risk beliefs are distinct from privacy beliefs, and studies have examined their relationships [e.g., Okazaki et al., 2009]. To prevent any confusion, those studies without a privacy construct are excluded.

Finally, only peer-reviewed academic research is analyzed for improved rigor. Potential contributions from professional journals and magazines [e.g., Brown, 2009] are discussed later. This research adopts a normative approach to studying privacy concerns [Smith et al., 1996] in order to present a unified view of the construct, the limitation of which is also discussed later.

Journal Pool, Search Strings, and Time Range

The primary source of publications consists of IS journals, as IS is a major discipline in this area of research; the Association for Information Systems (AIS) website (www.aisnet.org) hosts a list of the journals. Nevertheless, not all the IS journals were searched, as some seldom publish on empirical behavioral studies, such as *Artificial Intelligence*, *IEEE Transactions on Software Engineering*, and *Computer and Operations Research*. Other IS journals that have been searched in this study are reported in Table 2. In addition, the bibliographies provided by Davison et al. [2003] and Chan et al. [2005] both indicate that many other disciplines in business, psychology, and social sciences are also involved in privacy research. To incorporate findings from these disciplines and to provide a comprehensive synthesis on the topic, journals from other disciplines were also searched, majorly through online research databases such as EBSCO/Business Source Premier and ScienceDirect. The third source includes the proceedings of the International Conference on Information Systems (ICIS), which publish high quality research articles in the IS field [Koh, 2003].

Next, search strings used to retrieve articles from the journal pool, especially the searchable online databases, were selected. Although “privacy concerns” and “information privacy” are popular keywords, an analysis on example articles from leading IS journals reveal that not all the studies have used either keyword. Indeed, other keywords were used, such as online privacy, consumer privacy [Awad and Krishnan, 2006], privacy calculus [Dinev and Hart, 2006], privacy assurance, privacy statement, privacy seal [Hui et al., 2007], and simply, privacy [Stewart and Segars, 2002]. Other papers contain no keywords related to “privacy,” but the term appeared in the titles or abstracts [e.g., Kim, 2008; Yao and Murphy, 2007]. Therefore, to maximize the coverage of qualified articles, the term *privacy* is searched in titles, abstracts, and keywords. Details of the search process are described later.

While there is no particular guideline for specifying the time range of the publications, a typical approach is to recognize a historical fact in the line of research [Lee et al., 2007]. Using this method, this study sets 1996 as the starting point because of Smith et al.’s [1996] influential work of developing a scale to measure the privacy concern construct. There are several reasons. First, studies on information privacy prior to 1996 had been focused on employee privacy within organizations [e.g., Woodman et al., 1982]. With the proliferation of the Internet technology, information privacy is becoming more critical in the online environment. Second, e-commerce emerged in the mid-

1990s, and the number of corresponding research articles substantially increased since 1996 [Lee et al., 2007; Ngai and Wat, 2002]. As the review focuses on online information privacy research, it is acceptable to treat Smith et al.'s work as a critical milestone in this area and 1996 as the starting point of literature search. In addition, the search process, starting from the most recent publications, indicates that a small number of articles published prior to 2000 meet the inclusion criteria, further confirming the choice. Therefore, the author searched for articles published since 1996.

The Search Process

A variety of channels were used to find qualified articles from the above journal pool. For the IS journals, a combination of publishers' websites, electronic publications, and printed publications was used. ICIS proceedings were searched directly from the AIS website.

Articles from other disciplines were extracted from online databases (EBSCO/Business Source Premier and ScienceDirect); printed publications were consulted whenever the digital subscription does not contain the full text. In both online databases, the author searched for the string "privacy" in the titles, abstracts, and keywords in articles published since 1996. For EBSCO, additional limiters such as "peer-reviewed academic journals and research articles" were used, yielding a list of 3,911 articles. The list was sorted on sources (publication names) with fifty articles shown on each page. Many sources were skipped that do not have a tradition of publishing empirical behavioral studies, such as the *Journal of the American Association of Individual Investors (AAII)* and the *American Bankers Association (ABA) Journal* that appeared on top of the list. The rest of the list was scrutinized carefully. For ScienceDirect, the search was restricted to journals in the following fields: business, management, and accounting; decision sciences; psychology; and social sciences. The search yielded 949 papers, many of which were published in journals such as *Computer Law & Security Review* (146 papers) and *Computer Standards & Interfaces* (forty-three papers) and were discarded due to limited relevance to the study. The remaining 452 articles were examined based on criteria in Table 1.

Through the above process, eighty-eight articles were recognized from the journal pool, including fifty-five articles from IS journals, six from ICIS proceedings, and twenty-seven from other disciplines. The distributions of the articles are shown in Table 2.

Table 2: Publications by Academic Fields

Academic fields	Number of articles
Information Systems (IS)	<u>55</u>
10 IS journals with the most publications:	
MIS Quarterly	6
Decision Support Systems	5
Journal of Internet Commerce	5
Computers in Human Behavior	4
Communications of the Association for Information Systems	3
European Journal of Information Systems	3
Information Systems Research	3
International Journal of Electronic Commerce	3
Journal of the Association for Information Systems	3
Other IS journals	20
Marketing and consumer research	14
Other management fields (including tourism management, service management, healthcare management, engineering management, and organization science)	12
Psychology	1
ICIS proceedings	6

Note: Other IS journals with no qualified papers recognized (since 1996) include *Communications of ACM*, *Information and Organization*, *Information Systems Journal*, *Information Technology and People*, *International Journal of Information Management*, *Journal of Information Systems*, *Journal of Information Technology*, *Journal of Information Technology Theory and Application*, *Journal of Organizational Computing and Electronic Commerce*, and *MIS Executive*.

Unit of Analysis and Coding

The unit of analysis in this research contains constructs and their causal relationships. The following items were recorded: privacy constructs, antecedents, consequences, and moderators. The measurements of the privacy constructs were also recorded. For the causal relationships and moderating effects, the study recorded the effect sizes (e.g., path coefficients, correlations, t-values, and F-values, etc.) and the significance levels if available, and narrated the major findings in each study. To provide more information about the literature, the following contents were also recorded: research objectives, research methods, samples and sample sizes, and data analysis methods. The coding results were categorized based on the natures and the interrelationships of the constructs, including antecedents, consequences, and moderating effects, reported in Appendices A, B, C, and D.

A typical threat to content analysis is the subjectivity in interpreting the contents, which is measured as the inter-rater reliability [Kassarjian, 1977; Neuendorf, 2002]. Nevertheless, since this review examines manifest content in each article rather than latent content derived from the words, the inter-rater reliability is not a critical concern [Potter and Levine-Donnerstein, 1999]. In addition, all the coding results are reported in the appendices for further verification. Therefore, despite the single rater in the study, the content recorded is reliable.

III. RESEARCH FINDINGS

Primary findings from the content analysis are reported in this section, including general descriptions of the sample of studies, a comparison of measurement scales, and categorized antecedents, consequences, and moderating effects.

Descriptive Results

Table 2 confirms the active roles of the IS discipline in studying online information privacy. Of the eighty-two journal articles recognized, fifty-five (or 67 percent) were published in IS journals; this is followed by the marketing and consumer research field (fourteen articles or 17 percent). In addition, information privacy research has been broadly embraced in the IS field, as illustrated by the variety of publication outlets. Surprisingly, not many empirical studies were recognized in the psychological field. This may be interpreted by the fact that privacy is more of a social and legal issue than a personal psychological issue, as evidenced by the number of publications in journals such as *Computer Law & Security Review*.

Academic research on online information privacy has gained popularity in the last decade, as shown in Figure 1. Interestingly, except for Smith et al.'s [1996] study, no qualified research was published prior to 1999. This conforms to Lee et al.'s [2007] finding that it typically takes time before the academic literature recognizes the significance of practical developments in the e-commerce area.

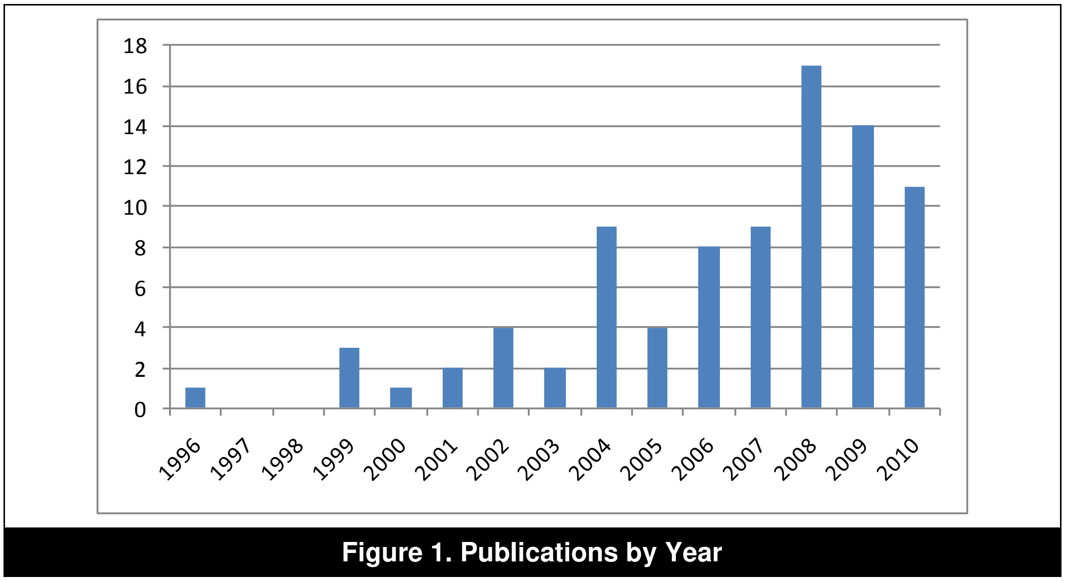

Figure 1. Publications by Year

In terms of research methods, surveying dominated the sample of studies (sixty-three studies or 72 percent), with the remaining based on experimentation and quasi-experimentation (twenty-five studies or 28 percent). Many of the survey studies tested individuals' privacy concerns with regard to general Internet use [e.g., Dinev and Hart, 2004, 2005, 2006], while experimental studies examined privacy concerns for specific websites [e.g., Bansal et al., 2008, 2010]. This seems to reflect the relative advantage of a method over the others in dealing with particular types of privacy concerns.

For data analysis methods, half of the studies (forty-four) applied the Structural Equation Modeling (SEM) approach, including the component-based SEM (PLS) and the covariance-based SEM (LISREL). Other methods were also used, including analysis of variance, analysis of covariance, multivariate regression, t-test, and correlations, etc. This implies the maturity of research methods in the area.

For the research subjects, over half of the studies (forty-five) explicitly stated that students (across all levels) were employed, although several studies did not provide subject profile information. While the potential limitations of using student subjects in research were noticed, as students comprise a major body of Internet users, their privacy perceptions were valid sources for privacy research [Junglas et al., 2008; Kumar et al., 2008].

In addition, a substantial number of studies (more than forty-one or 47 percent) were conducted on subjects in the United States, while several other studies did not provide the nationality information of the subjects. This suggests that the current understanding of online privacy concerns is primarily derived from the U.S. population. Scholars showed the difference in privacy perceptions between the U.S. citizens and non-U.S. citizens [Dinev and Hart, 2006] and the impact of culture and regulatory structures on privacy [Bellman et al., 2004]. It is critical to expand research on other populations in such a globally networked society.

For the privacy constructs studied, privacy concern dominated the sample of studies (seventy articles or 80 percent), followed by perceived privacy. A few other constructs were used occasionally, such as perceived privacy risk likelihood [Cazier et al., 2008], and privacy attitude [Stutzman et al., 2011]. Shown in Appendices A and B and discussed later, no significant difference was observed between the constructs in terms of antecedents and consequences, confirming the validity in the literature search.

The review also showed distinctions in the conceptualizations and measurements of the privacy constructs, especially the privacy concern construct. Several studies were devoted to developing scales to measure it. Due to the potential impact of measurements on theories, it is necessary to compare the existing scales, discussed in the next section.

Information Privacy Concerns: Conceptualizations and Measurements

While companies such as Equifax use a general, one-item scale to measure information privacy concerns [Smith et al., 1996, p. 185], scholars tend to interpret it as a latent construct and measure with manifest variables. Due to the differences in conceptualizations of the construct, several measurement scales were developed in the literature with many others adapted from past research. The review recognized five scales that were developed through a rigorous scale-development process to particularly measure the construct; key components of these scales are summarized in Table 3.

Table 3: Comparison of the Measurements of Information Privacy Concerns

Literature	Structure of the construct	Comments
Smith et al. [1996]	Four dimensions: collection (4 items), errors (4 items), improper access (3 items), and unauthorized secondary use (4 items)	These four dimensions are highly correlated, but a higher-order construct was not proposed.
Stewart and Segars [2002]	Second-order construct with four dimensions: collection (4 items), errors (4 items), unauthorized access (3 items), and secondary use (4 items)	This scale is based on Smith et al. [1996].
Malhotra et al. [2004]	Second-order construct with three dimensions: control (3 items), awareness (3 items), and collection (4 items)	The collection dimension overlaps with that in Smith et al. [1996] and Stewart and Segars [2002]
Dinev and Hart [2004]	Two dimensions: abuse (4 items) and finding (9 items)	Abuse deals with improper access and unauthorized use, and finding includes a number of specific privacy issues such as the exposure of names, address, and credit card information.
Buchanan et al. [2007]	Unidimensional (16 items)	The items measure a person’s concerns about specific privacy issues such as identity theft, access to medical records, virus attack, and mishandling of e-mails, etc.

The first study, by Smith et al. [1996], explored the underlying structure of privacy concerns and developed a latent construct called *Concerns for Information Privacy* (CFIP). CFIP consists of four dimensions: collection, errors, unauthorized secondary use, and improper access. Although these dimensions were highly correlated, Smith et al.

did not propose a higher-order construct. To enhance the psychometric properties of the scale, Stewart and Segars [2002] proposed a higher-order CFIP construct with the same dimensions and items, which provided a parsimonious view of the construct and received stronger theoretical as well as empirical support such as model fit. Although the original CFIP scale was not restricted to the Internet specificity, it has gained popularity in this area of research (see the third column in Appendix A).

Malhotra et al. [2004] developed another scale of privacy concerns from the Internet specificity, called Internet Users' Information Privacy Concerns (IUIPC). It is a higher-order construct with three dimensions: control, awareness, and collection. The rationale for developing a new scale other than CFIP was that the dimensionality of privacy concerns is "neither absolute nor static" and "the Internet provides a variety of means for consumers to control personal information that is stored in an organization's database" [Malhotra et al., 2004, p. 338]. However, no evidence shows the limitations in measuring Internet privacy concerns with CFIP, and further research using this scale did not report noticeable problems [e.g., Angst and Agarwal, 2009; Kumar et al., 2008]. Nevertheless, the IUIPC construct suggests new ways of conceptualizing and measuring the privacy concern construct.

The fourth scale, by Dinev and Hart [2004], was also developed in the Internet domain with modifications needed to avoid capturing unrelated beliefs. Two dimensions of privacy concerns were identified: finding and abuse. These two dimensions deal with privacy concerns regarding specific issues such as the theft of credit card information and personal contact information. Although the two dimensions were highly correlated, Dinev and Hart did not propose a higher-order construct, either.

The last scale, by Buchanan et al. [2007], contains sixteen unidimensional items that capture specific privacy issues, which are comparable to the items developed by Dinev and Hart [2004].

Comparing across the scales in Table 3, one may notice that although the specific structures of the scales differ, they share many common items or dimensions. While the Smith et al. scale, further refined by Stewart and Segars, was the most adopted, the existence of other scales and the rationales of developing those scales suggest that refinement is needed to capture the most relevant components of the CFIP construct in an evolving technological, social-cultural and legislative environment [Dourish and Anderson, 2006]. It would also be important, from a research rigor point of view, to test the construct validity of the scales across studies.

Although some studies adopted the full scales listed above [e.g., Angst and Agarwal, 2009; Bellman et al., 2004; Kumar et al., 2008; Van Slyke et al., 2006], others tailored the measures to fit particular research contexts [e.g., Faja and Trimi, 2006; Pavlou et al., 2007; Sheng et al., 2008]. A key rationale for modification, as mentioned above, was that it helped to avoid capturing unrelated sets of beliefs about privacy concerns. It was also not uncommon for studies to use surrogates to measure privacy perceptions, such as information privacy anxiety, information privacy exposure, perceived information privacy importance [Chai et al., 2009], perceived privacy control [Connolly and Bannister, 2007], and perceived importance of personal privacy [Hossain and Prybutok, 2008]. Many of these measures, though, share essential aspects of privacy concerns with existing scales and provide important supplements to these scales. To sustain the research tradition in this area, it would be beneficial to refine existing scales to incorporate the additional facets of the privacy concern construct.

Antecedents of Privacy Concerns

To date, multiple theories were applied to interpret the formation of individuals' privacy concerns and to analyze the corresponding behavioral consequences, such as the expectancy theory [Hann et al., 2007], information boundary theory [Xu et al., 2008], personality theory [Korzaan and Boswell, 2008], principle-agent theory [Pavlou et al., 2007], privacy calculus theory [Dinev and Hart, 2006], procedural fairness theory [Culnan and Amstrong, 1999], protection motivation theory [Chai et al., 2009], social cognitive theory [Chai et al., 2009], social contract theory [Malhotra et al., 2004], and social response theory [Zimmer et al., 2010]. A large number of antecedents were studied based on the theories. These factors, as shown in Appendix B, can be categorized into five groups based on their levels of research: individual factors, social-relational factors, organizational and task environmental factors, macro-environmental factors, and information contingencies. A summary of these factors follows.

Individual Factors

The individual-level factors are thus far the most frequently analyzed antecedents of online privacy concerns. Based on the natures and the theoretical backgrounds of the factors, they can be further categorized into the following groups:

Demographic factors Age, gender, education, income, and other individual factors are expected to have a potential impact on individuals' privacy concerns. A frequently studied factor, gender, seems to exert a relatively consistent effect on privacy beliefs: except for a few studies in which insignificant effect was observed [e.g., Ji and Lieber, 2010; Yao et al., 2007], others show that women are in general more concerned about their information privacy than men [Fogel and Nehmad, 2009; Hoy and Milne, 2010; Janda and Fair, 2004; Joinson et al., 2010; Laric et al., 2009; Sheehan, 1999; Youn, 2009]. Age has a positive impact on privacy concerns in some of the studies [Janda and Fair, 2004; Joinson et al., 2010; Laric et al., 2009], but in others it influences only those without online shopping experiences [Chen et al., 2001b]; for individuals in different cultural, economic or technological environments, age may have an opposite impact on privacy concerns [Zhang et al., 2002]. Other factors, such as income and education, were not found to have a significant impact on privacy concerns across studies [Chen et al., 2001b; Ji and Lieber, 2010; Zhang et al., 2002].

While the above studies formally tested the direct impact of consumer demographics on privacy beliefs, others have operated these factors as control variables and observed similar effects [e.g., Bellman et al., 2004]. In addition to the predictive effects, demographic factors such as gender were also found to have a moderating impact on privacy concerns [Janda, 2008], although this type of research is very limited.

Several studies provide explanations of why demographic factors influence a person's privacy concerns. For example, Chen and Rea [2004] suggest that, compared to women, men have stronger interests and skills in computers and are more likely to take active control over unwanted presence. Similarly, Fogel and Nehmad [2009] explain that men are more prone to risk-taking than women. These arguments suggest that a person's knowledge, experience, and even personality traits are closely related to his/her levels of privacy concerns.

Personality traits As a part of the scale development process, Smith et al. [1996] tested the impact of paranoia (defined as the persistent misperception of oneself as the target of another's thoughts or actions; Fenigstein and Vanable, 1992), social criticism (defined as the degree of acceptance or rejection of the values, norms, and practices of society; Jessor and Jessor, 1977), and cynical distrust (standing for the distrust of apparent motives of others) on CFIP; correlation analysis showed a positive link of each trait to CFIP. Dinev and Hart [2005] then examined the impact of social awareness (referring to a citizen's behavior with respect to following and being interested in and knowledgeable about community and government policies and initiatives, including those related to technology and the Internet) on Internet privacy concerns and found a positive relationship.

Two studies so far tested the impact of the Big Five personality traits [McCrae and Costa, 1991] on privacy concerns: the study by Junglas et al. [2008] shows that agreeableness (defined as an individual's propensity to strive for harmony and low levels of conflict in interpersonal relationships) has a negative impact on CFIP, while conscientiousness (defined as an individual's strive for dependability, attention to detail, and exact effort) and openness to experience (defined as an individual's curiosity, intellect, and propensity to try new things and to experience new situations) both have a positive effect. The other two traits, extraversion (defined as an individual's predisposition to experience positive life events) and emotional stability (defined as an individual's tendency to stay emotionally balanced across situations), have insignificant impacts on CFIP. The other study by Korzaan and Boswell [2008], however, shows different results: agreeableness had a positive impact on CFIP; extraversion and conscientiousness had no significant impact; and neuroticism and intellect were found to influence computer anxiety, but their impacts on CFIP were not tested. Although further research is needed to resolve the conflicts, the literature confirms that certain aspects of personality traits do have an impact on a person's privacy concerns.

Personal knowledge and experience Personal knowledge and experience are important sources of information about privacy issues. These include general knowledge about Internet use and specific knowledge about privacy invasions. Empirical evidences of the impact of specific knowledge and experience on privacy concerns are relatively consistent, as previous experience with information misuse and disclosure [Smith et al., 1996; Okazaki et al., 2009], knowledge of media coverage on information misuse [Smith et al., 1996], and previous experience with online privacy invasion [Bansal et al., 2010; Zviran 2008] all have a positive impact on privacy concerns. Mixed effects were found regarding general knowledge and experience: Internet literacy [Dinev and Hart, 2005] and Internet experience [Bellman et al., 2004] were shown to have a negative impact on privacy concerns; Web usage and use of privacy enhancing mechanisms [Zviran 2008] had a positive impact; Web skills and Web experience had no impact [Janda and Fair, 2004; Zviran 2008]; and Internet use fluency and Internet use diversity both had a mixed impact on privacy concerns [Yao et al., 2007; Yao and Zhang, 2008]. A possible reason for the mixed results is the variety of Internet knowledge, which may have distinct roles in privacy formation. Another reason is that the relationship between general knowledge of Internet and privacy concerns may not be linear: as the knowledge of privacy issues grows, a person may become more concerned about online privacy; with further accumulation of such knowledge, the person may learn to avoid some of the privacy risks and therefore become less concerned. More efforts are needed to examine the nature of such knowledge and its impact on privacy concerns.

Psychological and social-psychological factors A person's online privacy concerns may be influenced by other psychological or social-psychological states of the person. For example, Yao et al. [2007] studied the impacts of psychological need for privacy (or privacy disposition, defined as an individual's disposition to desire more or less privacy in various social situations) and beliefs in privacy rights on online privacy concerns; the empirical results confirmed the impact of both. Xu et al. [2008] tested the roles of privacy disposition, although its impact on privacy concerns was mediated by another construct called *perception of intrusion*. Phelps et al.'s [2001] analysis of consumers' desire for control over personal information also shows that this construct has a positive impact on privacy concern.

Stewart and Segars [2002] analyzed the influence of computer anxiety on CFIP and observed a positive relationship between the two. Computer anxiety denotes the tendency of individuals to be uneasy, apprehensive, or fearful about current or future use of computers [Parasuraman and Igbaria, 1990]; individuals who experience high levels of computer anxiety are likely to behave less comfortably around computers than individuals whose level of anxiety is low, therefore having more concerns about the collection and use of their private information through computers. The study by Korzaan and Boswell [2008], though, did not find support of this relationship, for which the reasons were discussed.

Self-efficacy, referring to a person's belief in his or her capabilities and cognitive resources needed to perform certain tasks [Bandura, 1994], is another potential predictor of privacy concerns. The study by Yao et al. [2007] found marginal support of the impact of general self-efficacy on privacy concerns, although the influence of the more pertinent computer self-efficacy construct was not tested. Due to the close relationship between computer self-efficacy and computer anxiety [Igbaria and Ilvari, 1995; Thatcher and Perrewe, 2002], one would expect that computer self-efficacy would have a stronger impact on privacy concerns than general self-efficacy, which needs to be further verified.

Dinev and Hart [2004] tested the impact of perceived vulnerability and perceived ability to control on privacy concerns; only the impact of perceived vulnerability was confirmed. The studies by Xu [2007] and Xu et al. [2008], though, found strong support of the impact of perceived control on privacy concerns. A similar construct, decisional control, was also found to have a significant impact on privacy concerns [Chen et al., 2009].

Finally, perceived Internet privacy risks [Dinev et al., 2006; Dinev and Hart, 2006; Xu et al., 2008] and trust beliefs [Pavlou et al., 2007] both have a significant impact on privacy concerns: the former increases a person's privacy concerns while the latter mitigates the concerns. A potential relationship between these two antecedents was tested in literature, showing that trust belief is negatively associated with risk belief [e.g., Xu et al., 2005]. It should be noted that based on the definitions, perceived vulnerability and perceived privacy risk are equivalent concepts [Dinev and Hart, 2004; Youn, 2009].

Social-Relational Factors

These factors gauge the influence of people one knows on his/her awareness of privacy issues. For example, Xu et al. [2008] tested the indirect impact of social norms (also called subjective norms, referring to the common patterns and forms of privacy in a social group that the individual belongs to) on individuals' privacy concern, which was mediated by privacy disposition. Another study by Youn [2008] examined the influence of parental mediation on teens' privacy concerns. Of the three mediation techniques studied, co-surfing and parent-child discussion had positive impacts on privacy concern, and rule-making had no significant impact. Other social-relational factors such as peers' impact on privacy invasion and protection were also studied [Chen et al., 2009], although specific antecedents of privacy concern were not recognized. Overall, studies on this type of antecedents are limited and demand more attention.

Organizational and Task Environmental Factors

Privacy concerns are largely due to improper information practice by organizations, so that organizations play critical roles in influencing consumers' concerns. A popular approach to alleviating privacy concern is to establish and enforce privacy policies and fortify the policies with third party assurance. A number of studies have tested the impact of both, and the results are in accordance with the expectations [Andrade et al., 2002; Lee and Cranage, in press; Lwin et al., 2007; Nam et al., 2006; Wirtz et al., 2007]. Other types of Web vendor privacy interventions, representing the level to which a specific website conveys its efforts to address privacy issues and discloses the company's information practices, were also found to have an impact on privacy perceptions [Faja and Trimi, 2006].

Online merchants may adopt other techniques to reduce uncertainties in a virtual environment. Two techniques, social presence and website informativeness, could achieve this result [Pavlou et al., 2007]. The former refers to the extent to which a consumer feels that the online environment closely resembles a physical interaction with a seller and recreates the notion of human touch, and the latter represents the degree to which a consumer perceives that a website provides resourceful and helpful information about the seller. Both help to reduce the privacy concerns about a particular website.

In addition, the reputation and trustworthiness of an organization also reduce a person's privacy concerns regarding that organization [Andrade et al., 2002; Yousafzai et al., 2009], and reputation has an impact on trust beliefs as well [Eastlick et al., 2006]. However, the impact of reputation on privacy concerns was not supported in Nam et al.'s [2006] study.

Macro-Environmental Factors

Two environmental factors, cultural values (e.g., power distance, individualism, masculinity, and uncertainty avoidance; Hofstede, 1991] and governmental regulatory structures (e.g., omnibus, sectoral, or non-regulation/self-help), were tested for their impact on privacy concerns. The study by Milberg et al. [2000] confirmed the impact of cultural values on Internet users' information privacy concerns: power distance, individualism, and masculinity each have a positive impact on the concerns, whereas uncertainty avoidance has a negative impact. A study by Bellman et al. [2004] showed a complex relationship between the cultural dimensions and the CFIP dimensions, and this relationship is further mediated by government regulations.

The relationship between governmental regulatory structure and CFIP was also tested: Bellman et al. [2004] showed that people from countries with no privacy regulation were more concerned about errors in databases and online transaction security than people from countries with omnibus or sectoral regulations. On the other hand, Milberg et al. [2000] showed that higher-level privacy concerns were associated with the preference for more restrictive regulatory approaches than corporate self-regulation, implying that more restrictive regulations are helpful in reducing such concerns. Other studies also confirmed the roles of government regulations on privacy belief [Lwin et al., 2007; Tsarenko and Tojib, 2009; Wirtz et al., 2007].

Information Contingencies

Studies show that people are more sensitive to the requests of certain types of information than other types [e.g., Rohm and Milne, 2004]; these factors are called information contingencies in this study. Two forms of information contingencies are examined, as summarized below:

Types of information A number of studies tested the impact of requests for certain types of information on individuals' privacy concerns: Rohm and Milne [2004] showed that people were more concerned about their medical records when such information was used by other organizations, especially by those contacted less frequently; Ji and Lieber [2010] showed that online disclosure of personal identifiable information such as homework address and video was significantly associated with privacy concerns; and Ward et al. [2005] showed that a person's privacy concern was associated with financial information requests but not with requests for personally identifiable information. Another research by Faja and Trimi [2006] examined the moderating role of identifiable information and non-identifiable information on the relationship between privacy and behavioral intentions and yielded positive outcomes.

While certain rules of thumb may be derived from the studies, some scholars argue that the rules may not hold universally [Zimmer et al., 2010], and no existing criteria are applicable to many other types of information not analyzed in the literature. For instance, would a Facebook-user worry about the information privacy regarding his/her list of favorite restaurants and music records? Information boundary theory [Stanton and Stam, 2003] indicates that the perception of information privacy is not fixed but influenced by contextual factors such as interpersonal relationships. This suggests that a focus on information types may not produce generalizable results. A more pertinent approach is needed.

Information sensitivity Moving beyond information types, other research used various forms of information sensitivity measures to test the impact of information requests on privacy concerns. For example, Rohm and Milne [2004] used the information sensitivity concept to develop their research model, and Malhotra et al. [2004] used a dichotomy to examine the impact of less sensitive information and more sensitive information on trust belief and behavioral intention. Although the impact of the information did not fall directly onto the privacy constructs, Malhotra et al. implied in their discussion a potential relationship between the two. Yang and Wang [2009] conducted a research to directly test the impact of information sensitivity on privacy concerns; the results were however insignificant. Bansal et al. [2010], then, experimentally tested the impact of perceived health information sensitivity on individuals' health information privacy concerns and observed a significant relationship.

Using an information relevance measure, Lwin et al. [2007] found that people's privacy concerns are dependent on the relevance of data to online transactions, and their concerns will rise if irrelevant data are requested. Information exclusivity, referring to the kind of information about a specific person, was also found to have an influence on privacy concerns [Chen et al., 2009]. Although information sensitivity seems to be a key to understanding the impact of information on privacy, as this construct has been traditionally underdeveloped [Zimmer et al., 2010], the limited empirical evidence suggests that more research is needed to test the relationship in order to reach a consensus.

In sum, many privacy concern antecedents were recognized in the literature. Although the results are mixed for certain factors, in general a person's concerns for information privacy are dependent on a number of factors ranging from individual characteristics to information contingencies. It would be important to clarify the mixed effects of some critical antecedents such as personal knowledge and experience, and to recognize additional factors from the multiple levels.

Consequences of Privacy Concerns

The consequences of privacy concerns also received substantial attention in research, as shown in Appendix C. Many of the consequence factors were analyzed from the theory of reasoned action [TRA; Ajzen and Fishbein, 1980] and the theory of planned behavior [TPB; Ajzen, 1991] perspectives, including beliefs of the behavior, attitudes toward the behavior, behavioral intentions, and actual behaviors. These categories of factors are summarized in sequence.

Personal Beliefs

Trust belief Trust belief refers to the degree to which people believe a firm is dependable in protecting consumers' personal information [Malhotra et al., 2004]. It differs from other types of beliefs such as disposition to trust and institution-based trust [McKnight and Chervany, 2002]. The impact of privacy concerns on trust belief has been investigated in various contexts such as online textbook purchase [Liu et al., 2005; Van Slyke et al., 2006], online subscription [Eastlick et al., 2006], financial service [Casalo et al., 2007], healthcare [Bansal et al., 2010] and general online shopping [Chiu et al., 2009]. Most studies show a negative impact of privacy concerns on trust, although no impact and even positive impact were occasionally observed [e.g., Bansal et al., 2010; Van Slyke et al., 2006]. Possible reasons for the exceptions were discussed, pointing to a complex relationship between the constructs.

Risk belief and perceived uncertainty Another important consequence of privacy concern is perceived risk. Their relationship has been tested in similar manners as trust belief but the results are more consistent, showing that privacy concern has a positive impact on risk belief [Cocosila et al., 2009; Malhotra et al., 2004; Van Slyke et al., 2006]. The only exception is the second data set in Van Slyke et al.'s [2006] study, where non-significant relationship was observed for lesser known e-tailers.

Similar to risk belief, perceived uncertainty, referring to the degree to which the outcome of a transaction cannot be accurately predicted by the buyer due to seller and product related factors, is also positively related to privacy concerns [Pavlou et al., 2007].

Both trust belief and risk belief are important consequences of privacy concerns. The review shows that the extant literature presented controversial relationships between the factors, as trust belief and risk belief were also studied as antecedents of privacy concerns. This conflict is to be addressed later in the integrative framework.

Other personal beliefs Perceived importance of information transparency [Awad and Krishnan, 2006] and perceived usefulness to use firewalls to protect home computers [Kumar et al., 2008] are both significantly influenced by CFIP.

Attitudes

Both TRA and TPB indicate that attitude is the direct outcome of beliefs, which was analyzed in several studies in the review. Angst and Agarwal [2009], for example, studied the impact of CFIP on the likelihood of electronic health records adoption by customers; they found that CFIP had a positive impact on attitudes toward the adoption. Similarly, Cases et al. [2010] showed that perceived privacy had a positive impact on attitude toward a website, and Frye and Dornisch [2010] showed that privacy of medium had a positive impact on comfort of disclosing information via the medium. Ashley et al. [in press] found that privacy concern had a negative impact on customer relationship program receptiveness.

Exceptions were also observed. Kumar et al. [2008] did not find a significant impact of CFIP on individuals' attitudes toward using firewalls to protect home computers, although a positive impact of CFIP on the perceived usefulness of firewalls was observed. Krohn et al. [2002] found no impact of privacy concerns on attitude toward a website. The impact of privacy concerns on attitude toward online shopping was mixed in Lian and Lin's [2008] study. Further research is needed to clarify these results.

Behavioral Intention

Behavioral intention plays a critical role in human behavior [Ajzen, 1991; Ajzen and Fishbein, 1980]. Empirical studies in this area analyzed individuals' intentions to share information, to transact, and to take protective actions [e.g., Cheung and Liao, 2003; Dinev and Hart, 2005, 2006; Dinev et al., 2008; Eastlick et al., 2006; Korzaan and Boswell, 2008; Van Slyke et al., 2006; Smith et al., 1996; Stewart and Segars, 2002; Zimmer et al., 2010]. Other forms of intentions were also analyzed, such as opt-in intention [Angst and Agarwal, 2009] and intention to adopt personalized service [Sheng et al., 2008]. The general conclusion is that privacy concerns have a negative impact on the willingness to provide information for transactions and a positive impact on the intention to protect information privacy, with standardized path coefficients ranging from .107 to .710 (absolute values).

It should be noted, however, that the potential impact of privacy concerns on behavioral intention could be influenced by other factors, as Belanger et al. [2002] show that having a satisfying and pleasurable online experience drives purchase intention regardless of privacy and security concerns.

Actual Behaviors

A few studies moved forward to analyze the impact of privacy concerns on actual behaviors, including protective behaviors and transactional behaviors. For example, Son and Kim [2008] provided taxonomy of three categories and six types of privacy-protective responses, and tested the impact of information privacy concerns on these behaviors. The results showed that except for misrepresentation, privacy concerns had a positive impact on the other five types of behaviors, including refusal to provide information, removal of information, negative word-of-mouth, complaining to the company, and complaining to third parties. Lwin et al. [2007] showed that online privacy concern had a significant impact on information fabrication, technological protection, and information withholding. Another study by Zviran [2008] showed that privacy concern was positively associated with refraining of surfing; the other two types of protective behaviors, canceling online spending and reducing volume of online spending, were not significantly influenced by privacy concerns. The impact of privacy concerns on information disclosure in Hui et al.'s [2007] study, although negative, did not reach significance; in fact, most of the subjects in their study had low levels of privacy concerns. These results, compared to the significant relationship between privacy concerns and behavior intention, suggest that while people with more concerns about privacy are more careful about Internet use, they may still give up information for various reasons. This apparent cognitive dissonance is well discussed in psychological literature [Wood, 2000].

In sum, privacy concern has a significant impact on individuals' beliefs about information risks, attitudes toward information practice, behavioral intention to provide information or protect privacy, and actual behaviors. Academic research is needed to broaden the scope of these variables for an improved understanding of the behavioral consequences. Meanwhile, potential limitations of focusing on the privacy concern construct should be noticed: a few studies show that when information security perceptions were included in research, the impact of privacy factor became less significant and even non-significant [Janda, 2008; Kim, 2008; Kim et al., 2008b; Roca et al., 2009]. Although it is too early to draw the conclusion, research is needed to take this factor into account to specify an accurate role of privacy concerns in online behaviors.

Moderating Effects involving Privacy Concerns

A few studies examined the moderating roles of privacy concerns; Appendix D summarizes these findings. For example, Angst and Agarwal [2009] tested the impact of CFIP on a number of relationships in the adoption of electronic health records; the results showed a significant impact of CFIP on each of the relationships. Bansal et al. [2008] found empirical evidence of the impact of privacy concerns on the relationship between website design quality and trust of the website; the moderating role of consumers' privacy concerns on the adoption of opt-in/opt-out behaviors was also confirmed. However, the expected moderating effects on other relationships were not sustained [Luo and Seyedian, 2003].

On the other hand, factors that moderate the relationship between privacy concern construct and other factors were also examined, such as the type of information [Faja and Trimi, 2006], the context of information requests [Sheng et al., 2008], and gender [Janda, 2008]. It should be noted that although significant relationships were observed in the studies, the research on the moderating effects involving privacy concerns is still limited and more efforts are needed to further investigate these effects.

IV. DEVELOPMENT OF AN INTEGRATIVE FRAMEWORK

The above review recognized a large group of antecedents, consequences, and moderating effects related to privacy and privacy concern constructs. It is important to build a holistic view of these factors for further research and practice. Drawn upon TRA, an integrative framework for the study on online information privacy is developed in Figure 2. Key to the framework is the distinction between two types of information privacy concerns: General

Concerns for Information Privacy (or General CFIP) and Specific Concerns for Information Privacy (or Specific CFIP). The rationales of developing these two privacy concern constructs are discussed next, along with the propositions of some key relationships.

General CFIP versus Specific CFIP

Studies on information privacy concerns approach the construct from two broad perspectives: one captures general concerns for information privacy across contexts [e.g., Dinev and Hart, 2004, 2005, 2006], and the other captures specific concerns for information privacy in particular contexts [e.g., Pavlou et al., 2007; Van Slyke et al., 2006]. Various antecedents, such as macro-environmental factors and organizational factors, pose distinct impacts on these two aspects. To clearly specify the impact of the antecedents, this study adapts the research by Faja and Trimi [2006] to introduce the concepts of General CFIP and Specific CFIP. General CFIP refers to a person's overall concern for information privacy across e-commerce contexts. It measures a person's beliefs of the common practices of organizations in dealing with customers' private information. Specific CFIP, then, represents a person's privacy concerns in a given e-commerce context, such as information requests by a particular website. It measures a person's concerns about how the website may use his/her private information.

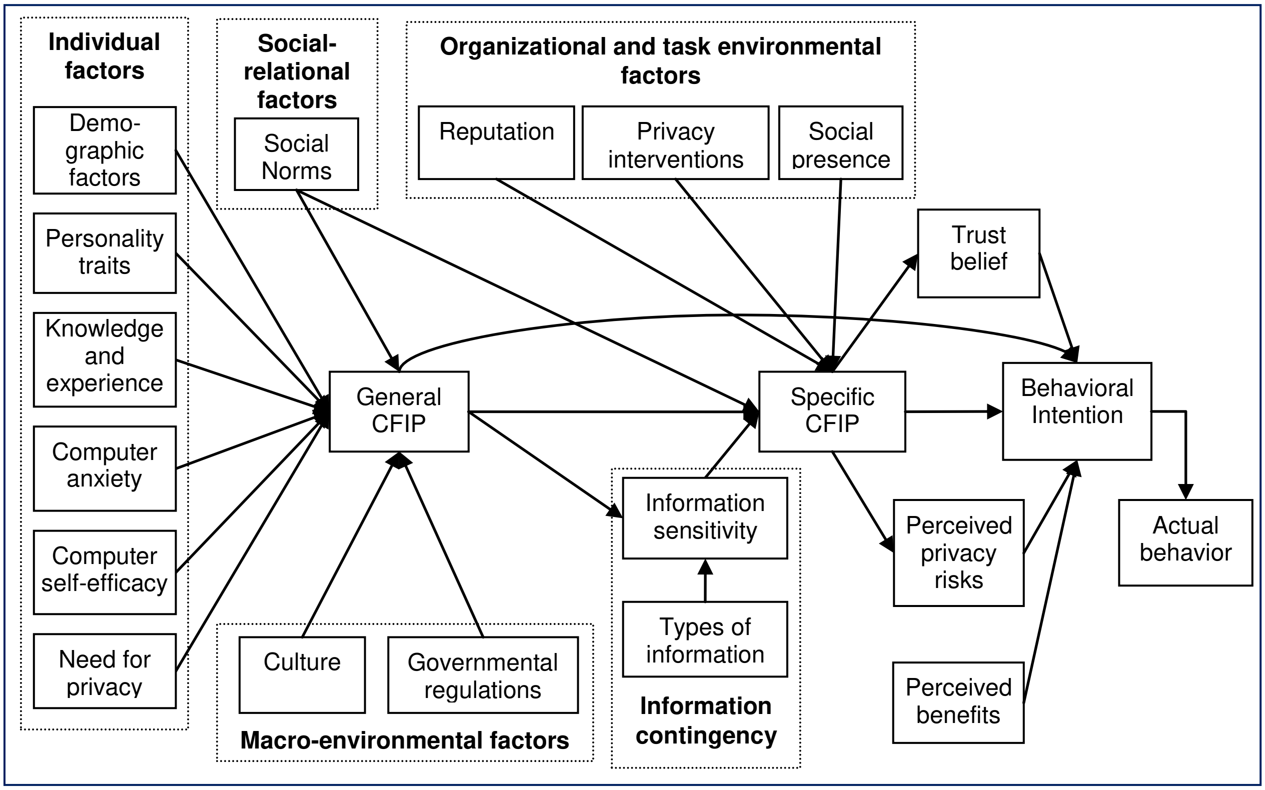

Figure 2. Integrative Framework for the Study on CFIP

The distinctions between general beliefs and specific beliefs were studied in other psychological areas such as self-efficacy (e.g., general computer self-efficacy versus software specific self-efficacy; Agarwal et al., 2000), anxiety (e.g., general anxiety versus computer anxiety; Brown et al., 2004), and self-esteem (e.g., general self-esteem versus specific self-esteem; Rosenberg et al., 1995). Studies show that general beliefs and specific beliefs are different phenomena and are not directly interchangeable: general beliefs are more relevant to the psychological wellbeing of a person (such as confidence, comfortableness, and anxiety, etc.), while specific beliefs are more relevant to the actual behavior [Rosenberg et al., 1995]. Although specific beliefs have an impact on the formation and adjustment in general beliefs [Chen et al., 2001a; Rosenberg et al., 1995], such impact is gradual and longitudinal, and general beliefs have an immediate impact on the formation of specific beliefs in a given context. For example, in computer mediated communication (CMC) a person's CMC anxiety is a proximal construct between general computer anxiety and the subsequent CMC attitudes and use [Brown et al., 2004]; in computer training, general computer self-efficacy does not have a direct impact on the training of a second software, but software specific self-efficacy does [Agarwal et al., 2000]. Both studies highlight the mediating roles of specific beliefs in behavioral motivations.

The distinction between General CFIP and Specific CFIP is helpful in clearly specifying the impact of various antecedents on privacy concerns and the impact of privacy concerns on subsequent behaviors: e.g., individual factors and macro-environmental factors are relatively stable across contexts, which may have a direct impact on General CFIP; organizational and task environment factors are context-specific, which may have a direct impact on Specific CFIP. Table 4 compares the two constructs; the statements are further examined in the following sections.

Faja and Trimi [2006] hypothesized that General CFIP would moderate specific privacy perception of a website; this effect was, however, invalidated by the experiment. This study suggests, in line with the above literature on the relationship between general beliefs and specific beliefs, that General CFIP is a direct antecedent of Specific CFIP. It is proposed,

Proposition 1: *A person's General CFIP is positively related to his/her Specific CFIP.*

Table 4: A Comparison Between General CFIP and Specific CFIP

	General CFIP	Specific CFIP
Domain of the construct	Concerning an individual's fundamental beliefs of information privacy across contexts.	Concerning an individual's attitude and belief about a particular information collection context (e.g., a particular website or company).
Emphasis of the construct	Emphasizing an individual's beliefs of how private information should not be handled in certain ways by e-commerce websites that collect such information.	Emphasizing an individual's perception of how private information could be improperly handled by the website that collects that information.
Consistency/stability	Stable across contexts; changing gradually overtime.	Contingent upon particular contexts; varying from site to site.
Potential antecedents	General CFIP is subject to the impact of fundamental, context-free antecedents such as personal attributes and macro-environmental factors.	Specific CFIP is subject to the impact of contextual factors associated with the website and the information collection context.
Potential consequences	General CFIP would have a direct impact on general protective behaviors (such as using firewall software or refraining from Internet use) and an indirect impact on behaviors toward specific websites.	Specific CFIP would have a direct impact on behaviors toward a particular website (such as information provision and transactions).
Relationship with each other	General CFIP influences the formation of Specific CFIP in a particular context.	The accumulation of Specific CFIP, in a long-run, will change the General CFIP; in a short-term, Specific CFIP would not change General CFIP substantially.

The following sections analyze the relationships between the two CFIP constructs and the antecedent and consequence factors reviewed. The literature provided detailed descriptions of most of the relationships, so that the emphasis is to clarify how these factors fit in the framework. The clarifications of some controversial relationships in the literature are also emphasized. It should be noted that although TRA posits attitude as a direct antecedent of behavioral intention, most of the literature reviewed in this study does not contain the attitude measure. To be consistent with the literature basis, the attitude construct is not included in the framework.

Impact of Individual Factors

Most of the individual factors are about fundamental traits of individuals, and the literature shows that their impacts on privacy concerns are irrelevant of contexts, suggesting an association with General CFIP. First of all, personal demographic factors and personality traits consist of stable characteristics and behavioral patterns of individuals that are independent of e-commerce contexts, suggesting that they influence General CFIP. Although some traits have an insignificant or mixed effect on privacy concerns, others such as gender, cynical distrust, paranoia, social criticism, and social awareness all have a strong impact.

Compared to the general knowledge and experience of Internet and Web, a person's knowledge and experience related to information privacy issues has a consistent impact on privacy concerns. Such knowledge and experience contains all prior understanding of the information privacy issues that have occurred, which is not restricted to a particular context and can be used as a reference for future information collecting activities, characterizing General CFIP.

Computer anxiety and computer self-efficacy deal with a person's comfort and capability in using computers and the Internet to finish transactions. Literature shows a positive impact of computer anxiety on CFIP [Stewart and Segars, 2002]. Since the literature typically measures computer anxiety as an individual-trait factor across computer usage contexts [Igbaria and Ilvari, 1995; Stewart and Segars, 2002; Thatcher and Perrewe, 2002], it suggests that this construct may have an impact on General CFIP. Due to the close relationship between computer self-efficacy and computer anxiety, a direct impact of computer self-efficacy on privacy concerns is also expected, although empirical studies are in need to test this relationship. The rationale is that a person of high computer self-efficacy would feel capable of handling information provision and privacy protection in the online environment; on the contrary, a person of low computer self-efficacy would feel uncertain about the potential risks of information privacy and incapable of adopting necessary techniques to protect it. Therefore, high computer self-efficacy will mitigate a person's concerns about information privacy, and low computer self-efficacy will raise the concerns. Similarly, the computer self-efficacy construct is generally measured as a context-free construct across application areas [Agarwal et al., 2000], so that it may have a direct impact on General CFIP only.

In addition, psychological need for privacy, or privacy disposition, is a context-free factor that represents a person's inclination to value privacy [Yao et al., 2007]. Although this factor was not widely discussed in literature, it addresses an important aspect of privacy concerns. In sum, many of the individual factors would have a potential impact on General CFIP, and it is proposed,

Proposition 2: Individual factors such as demographics, personality traits, knowledge and experience with regard to privacy issues, computer anxiety, computer self-efficacy, and the psychological need for privacy all have a significant impact on a person's General CFIP. Specifically, gender (women compared to men), age, personality traits (such as cynical distrust, paranoia, social criticism, and social awareness), privacy knowledge and experience, computer anxiety, and the psychological need for privacy all have a positive impact on General CFIP; computer self-efficacy has a negative impact on General CFIP.

Impact of Macro-Environmental Factors

Macro-environmental factors, including culture and governmental regulations, exert important impact on individuals' privacy concerns. As these factors are at the general environment level and are not unique to a particular organization, their potential impact falls onto General CFIP. For culture, the literature shows a complex relationship with privacy concerns, especially between the culture dimensions and the CFIP dimensions [Bellman et al., 2004; Milberg et al., 2000]. One possible reason is that both studies applied Hofstede's [1991] four-dimension model of culture, while other culture values and subcultures [Straub et al., 2002] were overlooked. Another reason is that the conceptualization and measurement of CFIP evolve over time with technological, social-cultural, and legislative environments, which also influence its relationship with culture. However, the literature agrees on the impact of certain culture dimensions on CFIP, especially power distance and individualism.

Governmental regulations also have a significant impact on privacy concerns: people in countries with limited legal protection are the most concerned and prefer more restrictive regulations, and the restrictive regulations help to reduce their concerns [Bellman et al., 2004; Milberg et al., 2000]. As governmental regulations regulate the general e-commerce environment, it is expected that they influence General CFIP only. It is proposed,

Proposition 3: Both culture values and governmental regulations have a significant impact on General CFIP. Specifically, cultural dimensions such as power distance and individualism have a positive impact on General CFIP, whereas governmental regulations have a negative impact on General CFIP.

Impact of Organizational Factors

Organizations are aware that customers would strike back on improper treatment of their private information, so they are implementing mechanisms to ensure fair information practices and reduce customers' concerns. One approach is to build the reputation of protecting privacy [Eastlick et al., 2006]. As reputation is an attribute of an organization, it has an impact on Specific CFIP only. Another approach to reducing customers' privacy concerns is to provide privacy-related interventions, such as website informativeness [Pavlou et al., 2007] that communicates information to customers regarding the approaches by the website to protect privacy. Faja and Trimi [2006] show that if a website is more open in its information practices and takes more measures to convey their dedication to privacy, customers would perceive fewer risks in disclosing information. Other interventions include privacy policies and third-party assurance. Social presence is the third approach recognized in literature for reducing privacy concerns, especially for online firms that lack the physical contact with customers [Pavlou et al., 2007]. Since the extent of social presence is determined by specific websites, it only influences Specific CFIP. Therefore, it is proposed,

Proposition 4: A firm's reputation to protect information privacy, its privacy-related interventions such as privacy policy, third party assurance, and website informativeness, and the social presence of the firm all have a negative impact on a person's Specific CFIP.

It should be noted that while some studies showed a positive impact of privacy policies on the willingness to provide information [Lwin et al., 2007; Meinert et al., 2006], others showed a non-significant impact on actual behaviors, as people rely more on legal protection than firms' self-regulations [Berendt et al., 2005]. More research is needed to provide additional evidence of the impact of privacy policy statements on CFIP.

Impact of Social-Relational Factors

Although the social-relational factors such as social norms and parental mediation are not widely discussed in literature, they are still important predictors of privacy concerns due to the influence of peers or family. Due to insufficient studies, it is unknown what particular influence one may receive from the social contacts: influence on general Internet use or on specific websites. Nevertheless, it is expected that both types of influences may exist, so that social norms may impact both types of CFIPs. As parental mediation is limited to teenage Web users, this factor is excluded from the framework. It is proposed,

Proposition 5: Social norms have a significant impact on both General CFIP and Specific CFIP.

Impact of Information Contingencies

The above review summarizes two information contingencies that may influence CFIP: types of information and information sensitivity. Although the direct impact of information types on CFIP was analyzed [e.g., Rohm and Milne, 2004], the mediating roles of information sensitivity has a stronger theoretical basis [Malhotra et al., 2004; Stanton and Stam, 2003] and is able to generate robust results; this study supports the latter view. While some types of information such as medical records may be sensitive for most people, other types of information may cause different extents of sensitivity for different people in different contexts, and only sensitive information may arouse a high concern. Such analysis also suggests that information sensitivity does not influence General CFIP but Specific CFIP, since the kind of information collected is best determined in a given context. It is proposed,

Proposition 6: Types of information collected from individuals have a strong impact on their perceptions of information sensitivity. Specifically, medical and financial information is more sensitive than contact information, and personally identifiable information is more sensitive than personally unidentifiable information.

Proposition 7: Perceived information sensitivity is positively associated with Specific CFIP.

Information sensitivity is not only determined by information types but also by other factors such as individual traits, culture and legislative environment [Bansal et al., 2010; Bellman et al., 2004; Xu et al., 2008], and it may also be subject to the impact of social norms. Instead of proposing a direct relationship between these factors, this study suggests that their relationships are mediated by General CFIP. Specifically, a person who is generally more concerned about online information privacy than others would be more sensitive to the request of the same piece of information. This, in addition to Propositions 2, 3 and 5 that predict a direct impact of individual factors, social norms, and culture and legislative factors on General CFIP, suggests a potential mediating effect [Baron and Kenny, 1986] of General CFIP. Therefore, it is proposed,

Proposition 8: General CFIP is positively associated with perceived sensitivity of the information collected.

The Consequences of Specific CFIP

Trust belief This framework addresses trust beliefs regarding specific websites; Internet trust [Dinev and Hart, 2006] is not discussed. Different individuals may develop drastically different beliefs about the trustworthiness of a given website, which help to alleviate their concerns about information privacy regarding that site [Van Slyke et al., 2006]. Many factors such as a firm's reputation, perceived security, social presence, privacy policies, and procedural fairness all influence the trust building process [Bansal et al., 2008; Casalo et al., 2007; Culnan and Armstrong, 1999; Eastlick et al., 2006; McKnight and Chervany, 2002; Pavlou, 2003], suggesting that trust is an overall evaluation of a firm after consolidating all other factors about the firm. Except for a few studies, many found a significant impact of CFIP on trust belief [e.g., Chiu et al., 2009; Eastlick et al., 2006; Liu et al., 2005; Malhotra et al., 2004]. It is therefore proposed, *Proposition 9: Specific CFIP about a website is negatively associated with the trust belief of the website.*

Perceived privacy risks Instead of measuring general Internet risks and uncertainties, this study addresses a person's perceived privacy risks with regard to a specific website. From the expectancy theory [Hann et al., 2007] and the protection motivation theory [Chai et al., 2009] perspective, a person who is concerned that his/her personal information may not be properly handled by an organization would anticipate certain risks and uncertainties regarding that information. Except for a few studies, most literature depicts CFIP as the antecedent of perceived privacy risks [e.g., Malhotra et al., 2004; Van Slyke et al., 2006], so that it is proposed,

Proposition 10: Specific CFIP about an organization is negatively associated with the perceived privacy risk regarding that organization.

Trust belief has a negative impact on perceived privacy risk, too [Malhotra et al., 2004; Van Slyke et al., 2006; Xu et al., 2005]. Since this relationship goes beyond the scope of the study, it is not discussed in this work.

Behavioral Intention To date, many different types of behavioral intentions were analyzed. Although it would be valuable to provide more detailed categorizations of the behavioral intentions and the corresponding behaviors, for which Son and Kim [2008] provide a preliminary frame, there exist many other types of behaviors and behavioral intentions that may not be properly categorized in the frame. For parsimonious purpose, these various types of behavioral intentions are broadly categorized into two groups: intentions to provide information for transactions and intentions to protect information. These types of behavioral intentions reflect a person's attitude toward the privacy protection by a website, so that Specific CFIP would have a potential impact on both types of intentions, well supported in the literature.

In addition to Specific CFIP, several other factors also have a potential impact on behavioral intention. Faja and Trimi [2006], for example, showed the direct impact of General CFIP on willingness to buy. In fact, when a person has limited knowledge about a website (such as during the first visit), he/she may have inadequate information to judge the Specific CFIP about the site, therefore relying on General CFIP to guide the behavior. In this case, General CFIP becomes a direct determinant of behavior.

Trust beliefs and perceived privacy risks are two other factors that have a potential impact on behavioral intention [e.g., Bansal et al., 2008; Malhotra et al., 2004; Van Slyke et al., 2006]. Although the literature implies that Specific CFIP would have a major impact on behavioral intention, trust beliefs and risk beliefs represent the psychological states aroused by Specific CFIP and would have an additional impact on behavior intentions, which were confirmed in several studies [e.g., Diven and Hart, 2006; Eastlick et al., 2006; Malhotra et al., 2004; Zimmer et al., 2010].

Finally, from the cost-benefit perspective, perceived benefit would have a potential impact on information disclosure intentions [Berendt et al., 2005], such as monetary and non-monetary benefits [Li et al., 2010], societal benefits [Son and Kim, 2008], compensations [Yang and Wang, 2009], and other benefits [Zimmer et al., 2010]. A categorization of the intrinsic and extrinsic motivations to disclose personal information was also provided [Tam et al., 2002]. Although the specific forms of benefits may differ, the literature suggests that perceived benefit helps to counterbalance the risk perceptions caused by privacy concerns, therefore motivating individuals to disclose information; in some circumstances perceived benefit may overwhelm the impact of CFIP [Awad and Krishnan, 2006; Hann et al., 2007]. Of course, the use of benefits should be appropriate, as rewards may sometimes inadvertently cause unnecessary concerns [Andrade et al., 2002]. It is proposed,

Proposition 11: Specific CFIP, General CFIP, and perceived privacy risk each have a positive impact on behavioral intentions to protect information and a negative impact on the intentions to provide information for transactions; on the contrary, trust belief and perceived benefit have a negative impact on behavioral intentions to protect information privacy and a positive impact on the intentions to provide information for transactions.

Actual Behavior The literature provides ample evidence of the impact of behavioral intention on actual behavior, so that it is proposed,

Proposition 12: Behavioral intentions such as the willingness to provide information for transactions and the willingness to protect information are positively associated with the actual behavior.

Moderating effects may also exist in Figure 2, based on the summary in Appendix D. However, those effects were not broadly analyzed in literature, and barely any effect was examined across studies. Therefore, the moderating effects are not proposed in the current research.

V. DISCUSSIONS AND CONCLUDING REMARKS

This research makes a number of contributions to the literature: it provides a comprehensive review of the empirical studies on online information privacy from the individual behavior perspective, building a holistic picture of the privacy concern construct and its associations with multiple antecedent and consequence factors. In addition, various measurements of privacy concerns are compared, showing the distinctions in conceptualizations and the need to refine the construct to capture its evolving nature. The propositions of General CFIP and Specific CFIP also help to discern privacy concerns within and across e-commerce contexts and function as the basis to classify the relationships with other factors. Finally, the review highlights issues in literature with regard to the causal relationships between trust belief, risk belief, and privacy concerns, and provides a preliminary solution.

A number of limitations in extant literature are recognized for further research, summarized as follows:

- The conceptualizations of the CFIP construct should be deepened to capture its evolving nature in a changing social-cultural, technological, and legislative environment.
- It is critical to gain deeper insight into privacy issues from countries other than the U.S. In addition to culture and regulatory structures, other factors such as privacy disposition, information sensitivity and social norms may also show significant distinctions across countries and should be studied more thoroughly.
- The conflicting effects of some individual-level antecedents, such as personality traits and personal knowledge and experience, should be clarified with cumulative research.
- Additional research should be conducted to understand how an e-commerce website may mitigate customers' privacy concerns via multiple interventions.
- The influence of social-relational factors should be further investigated due to the diffusion of social networking sites and online communities.
- Additional research should also be conducted to examine the impact of information sensitivity on privacy concerns and the antecedents of information sensitivity.
- The causal relationships between information privacy concerns, trust belief, and risk belief need to be further verified.
- More research should be devoted to understanding moderating effects involving privacy concerns.
- Finally, potential distinctions in privacy concerns with regard to different e-commerce models should be analyzed. The key issue to be considered is how individuals may respond differently to information requests from a transactional website and from a social-networking website.

Although this review develops an integrative framework for CFIP research based on in-depth analysis of literature, it would be necessary to test the framework empirically. The framework can be tested in a number of ways. First, it can be tested with surveys or experiments, and the difference is how the organizational/task environmental factors and information types are operationalized. To conduct a survey, subjects visiting different e-commerce websites should be identified in order to assess their perceptions of the organizational and task environmental factors; these subjects should also come from different cultural and regulatory backgrounds in order to test the effects of these macro-environmental factors. In addition, types of information requested by the sites should be measured in the survey. On the other hand, experiments may be conducted to manipulate the organizational/task environmental factors and information types. These two methods are deemed most sufficient but, indeed, most challenging due to the number of factors in the framework.

The second option to test the framework is to conduct meta-analyses on extant literature. Meta-analysis is an approach to cumulating results across studies on the same relationships to establish facts [Hunter and Schmidt, 2004], which has been broadly applied in the IS field. The difficulty is that some factors and relationships in the framework have not been analyzed in sufficient numbers of studies (such as the impact of culture on privacy concerns), which may threat the validity of this method.

The third option, which is recommended for further research, is to test the framework in blocks: the first block contains key constructs such as General CFIP, Specific CFIP, trust belief, risk belief, perceived benefits, behavioral intention, and actual behavior. This block is at the core of the framework. The second block contains General CFIP and its antecedents. The third block examines Specific CFIP and its antecedents, including General CFIP, social norms, organizational/task environment factors, and information contingencies. In other words, multiple antecedents in the framework may be tested based on their distinct impact on the intermediate variables such as General CFIP and Specific CFIP, which makes the empirical test of the framework feasible.

Implications of the Study

The study has implications for both research and practice. For research, it suggests that studies on online information privacy should explicitly indicate which type of privacy concerns, either General CFIP or Specific CFIP, is examined. This helps to clearly specify the impact of the antecedent factors and the effect on the consequence factors. In addition, if both content-free factors (such as individual characteristics) and context-specific factors (such as firm characteristics) are analyzed, it is important to incorporate both CFIP constructs in the study. This may help to improve the explanation power of the study, given the mediating roles of both CFIP constructs.

In addition, if types of information are examined in privacy research, it would be necessary to incorporate the information sensitivity measure in the study. As mentioned above, information sensitivity has stronger theoretical underpinning (such as information boundary theory; Stanton and Stam, 2003) than information types, which could help to discern the real perceptions of individuals in evaluating information requests.

Online firms today rely on customers' information to improve product offering and customer service. Although privacy concerns exist, key benefits that motivate consumers to disclose information should not be overlooked [Tam et al., 2002]. The framework shows that both Specific CFIP and perceived benefits have a direct impact on a person's behavioral intention to disclose information. This suggests, in accordance with past research [e.g., Berendt et al., 2005; Li et al., 2010; Yang and Wang, 2009], that, for firms to effectively persuade customers to give information, they should provide the kinds of benefits that match the privacy concerns.

In addition to enhanced benefits, an online firm may use a number of approaches to reduce customers' privacy concerns. Reputation, privacy interventions, such as privacy policy and website informativeness, and social presence, all provide customers opportunities to learn a firm's privacy practice. Firms should invest in multiple mechanisms to alleviate privacy concerns, to boost trust, and to reduce risk perceptions. They should also be careful in selecting the kinds of information requested from the customers, as irrelevant and sensitive information may cause more concerns than relevant and insensitive information. And finally, firms may use the influence of peers to address privacy concerns, as social norms may change a person's privacy belief. This is especially important when online consumers exchange ideas through online communities or social-networking sites. Firms may need to recognize the opinion leaders and work with them to address other customers' privacy concerns.

For individuals, the framework highlights multiple factors that influence their privacy-related behaviors. While legal protection and online firms' self-regulations may alleviate their concerns, online consumers may need to be equipped with necessary knowledge and skills to deal with privacy issues, to discern suspicious or unnecessary information requests, and to balance information privacy with benefits. Individuals may also gain knowledge from their peers regarding a particular company's privacy practice.

Limitations of the Study

A number of limitations in the current study are recognized. First, this review is based on empirical studies from the behavioral perspective; other studies such as conceptual framework and mathematical modeling were not included, which have contributions to privacy research as well. For example, Henderson and Snyber [1999] discussed three main driving forces of personal information privacy, including new technological capabilities, increasing value of information, and confusions surrounding ethical standards, and Prince and Barrett [2005] provided elaborate details of the relationship between technology innovation and privacy. Webster [1998] conducted a longitudinal case study to examine the impact of privacy on the use of desktop videoconferencing. Practitioners also contributed valuable solutions to privacy issues [e.g., Brown, 2009], from which new constructs may be developed to interpret privacy concerns. These studies should be incorporated in further research.

Second, this research is built solely on the privacy constructs. Many studies were conducted within the information privacy context without explicit notions of equivalent constructs [e.g., Cranor et al., 2007; Hann et al., 2007]. A review of those additional articles would be helpful in enhancing knowledge of information privacy and protection.

Third, the study treats perceived information privacy and information privacy concerns as alternative constructs based on a qualitative comparison of common antecedents and consequences. Whether these two constructs are effective substitutes is subject to further investigation. Two similar constructs, trust and distrust, for example, were shown to be non-substitutable [Lwicki et al., 1998].

Fourth, a focus on individuals' "perceptions" of information privacy may generate a slightly different view of the issue than a focus on "reality." Berendt et al. [2005] conducted an experiment to show that online users easily forget about their privacy concerns and communicate private information without any compelling reasons to do so. This suggests that although the perceived privacy concern is a major driver of behavioral intention, it would be necessary to measure the reality of privacy, especially for organizations and governments to develop effective policies and laws to protect information privacy.

Fifth, the review does not take into consideration the impact of perceived security on CFIP. As it was noted that perceived security may have a potential impact on CFIP and its relationship with other variables [Janda, 2008; Kim, 2008; Kim et al., 2008b; Roca et al., 2009], it is necessary to re-examine certain relationships in the framework with the existence of the security construct.

The normative approach in this study is another area of concern. Although this approach dominates privacy research, other perspectives are also helpful in broadening knowledge in this area [Smith et al., 1996]. Finally, the integrative framework contains many variables recognized in existing studies; it would be necessary, for theorizing purposes, to develop parsimonious models so as to simplify the framework and to recognize some robust relationships.

In conclusion, although studies on online information privacy concerns have made significant progress over the years, there are many uncharted areas to be explored. Scholars from various disciplines, especially IS, are expected to conduct further research to address the limitations recognized in this study and to promote the knowledge in this area to a higher level.

ACKNOWLEDGMENT

The author would like to thank the two anonymous reviewers for their insightful comments and suggestions for this article.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Articles preceded with an asterisk are included in the literature review.

Agarwal, R., V. Sambamurthy, and R.M. Stair (2000) "The Evolving Relationship Between General and Specific Computer Self-Efficacy—An Empirical Assessment", *Information Systems Research* (11)4, pp. 418–430.

Ajzen, I. (1991) "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes* (50)2, pp. 179–211.

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

Aljukhadar, M., S. Senecal, and D. Ouellette (2010) "Can the Media Richness of a Privacy Disclosure Enhance Outcome? A Multifaceted View of Trust in Rich Media Environments", *International Journal of Electronic Commerce* (14)4, pp. 103–126.

Allen, M.W. et al. (2007) "Workplace Surveillance and Managing Privacy Boundaries", *Management Communication Quarterly* (21)2, pp. 172–200.

*Andrade, E.B., V. Kaltcheva, and B. Weitz (2002) "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation", *Advances in Consumer Research* (29)1, pp. 350–353.

*Angst, C.M. and R. Agarwal (2009) "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion", *MIS Quarterly* (33)2, pp. 339–370.

*Ashley, C. et al. (In press) "Why Customers Won't Relate: Obstacles to Relationship Marketing Engagement", *Journal of Business Research*.

*Awad, N.F. and M.S. Krishnan (2006) "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization", *MIS Quarterly* (30)1, pp. 13–28.

Bandura, A. (1994) "Self-Efficacy" in Ramachaudran, V.S. (ed.) *Encyclopedia of Human Behavior, Volume 4,* New

York: Academic Press, pp. 71–81. Reprinted in Friedman, H. (ed.) *Encyclopedia of Mental Health* (1998), San Diego, CA: Academic Press.

*Bansal, G., F. Zahedi, and D. Gefen (2008) “The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation”, *Proceedings of the 29th International Conference on Information Systems*, Paper 7, pp. 1–9.

*Bansal, G., F. Zahedi, and D. Gefen (2010) “The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online”, *Decision Support Systems* (49)2, pp. 138–150.

Baron, R.M. and D.A. Kenny (1986) “The Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations”, *Journal of Personality and Social Psychology* (51)6, pp. 1173–1182.

Belanger, F., J.S. Hiller, and W.J. Smith (2002) “Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes”, *Journal of Strategic Information Systems* (11)3–4, pp. 245–270.

*Bellman, S. et al. (2004) “International Differences in Information Privacy Concerns: A Global Survey of Consumers”, *Information Society* (20)5, pp. 313–324.

Berendt, B., O. Gunther, and S. Spiekermann (2005) “Privacy in E-Commerce: Stated Preferences vs. Actual Behavior”, *Communications of the ACM* (48)4, pp. 101–106.

Brown, B. (2009) “Improving the Privacy and Security of Personal Health Records”, *Journal of Health Care Compliance* (11)2, pp. 39–68.

Brown, S.A., R.M. Fuller, and C. Vician, (2004) “Who’s Afraid of the Virtual World? Anxiety and Computer-Mediated Communication”, *Journal of the Association for Information Systems* (5)2, pp. 79–107.

Brutus, S., H. Gill, and K. Duniewica (2010) “State of Science in Industrial and Organizational Psychology: A Review of Self-Reported Limitations”, *Personnel Psychology* (63)4, pp. 907–936.

*Buchanan, T. et al. (2007) “Development of Measures of Online Privacy Concern and Protection for Use on the Internet”, *Journal of the American Society for Information Science and Technology* (58)2, pp. 157–165.

*Casalo, L.V., C. Flavian, and M. Guinaliu (2007) “The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking”, *Online Information Review* (31)5, pp. 583–603.

*Cases, A.S. et al. (2010) “Web Site Spill Over to Email Campaigns: The Role of Privacy, Trust and Shoppers' Attitudes”, *Journal of Business Research* (63)9–10, pp. 993–999.

*Cazier, J.A., A.S. Jensen, and D.S. Dave (2008) “The Impact of Consumer Perceptions of Information Privacy and Security Risks on the Adoption of Residual RFID Technologies”, *Communications of the Association for Information Systems* (23), Article 14, pp. 235–256.

Chai, S. et al. (2009) “Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens”, *IEEE Transactions on Professional Communication* (52)2, pp. 167–182.

Chan, Y. et al. (2005) “Information Privacy: Management, Marketplace, and Legal Challenges”, *Communications of the Association for Information Systems* (16), Article12, pp. 270–298.

Chellappa, R.K. and S. Shivendu (2007) “An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization”, *Journal of Management Information Systems* (24)3, pp. 193–225.

Chen, G., S.M. Gully, and D. Eden (2001a) “Validation of a New General Self-Efficacy Scale”, *Organizational Research Methods* (4)1, pp. 62–83.

*Chen, J. et al. (2009) “Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context”, *Proceedings of the 30th International Conference on Information Systems*, Paper 174, 1–18.

*Chen, K. and A.L. Rea, Jr. (2004) “Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques”, *Journal of Computer Information Systems* (44)4, pp. 85–92.

*Chen, J., Y. Zhang, and R. Heath (2001b) “An Exploratory Investigation of the Relationships Between Consumer Characteristics and Information Privacy”, *Marketing Management Journal* (11)1, pp. 73–81.

*Cheung, M.T. and Z. Liao (2003) “Supply-Side Hurdles in Internet B2C E-Commerce: An Empirical Investigation”, *IEEE Transactions on Engineering Management* (50)4, pp. 458–469.

*Chiu, C. et al. (2009) “Determinants of Customer Repurchase Intention in Online Shopping”, *Online Information Review* (33)4, pp. 761–784.

Ciocchetti, C.A. (2007) “E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors”, *American Business Law Journal* (44)1, pp. 55–126.

*Cocosila, M., N. Archer, and Y. Yuan (2009) “Early Investigation of New Information Technology Acceptance: A Perceived Risk–Motivation Model”, *Communications of the Association for Information Systems* (25), Article 30, pp. 339–358.

Conger, S. (2009) “Personal Information Privacy: A Multi-Party Endeavor”, *Journal of Electronic Commerce in Organizations* (7)1, pp. 71–82.

Connolly, R. and F. Bannister (2007) “Consumer Trust in Internet Shopping in Ireland: Towards the Development of a More Effective Trust Measurement Instrument”, *Journal of Information Technology* (22)2, pp. 102–118.

Cranor, L. et al. (2007) “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study”, *Proceedings of the 28th International Conference on Information Systems,* Paper 20, pp. 1–17.

*Culnan, M.J. and P.K. Armstrong (1999) “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation”, *Organization Science* (10)1, pp. 104–115.

Culnan, M.J. and C.C. Williams (2009) “How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches”, *MIS Quarterly* (33)4, pp. 673–687.

*Dai, H. and P.C. Palvia (2009) “Mobile Commerce Adoption in China and the United States: A Cross-Culture Study”, *The DATA BASE for Advances in Information Systems* (40)4, pp. 43–61.

Davison, R.M. et al. (2003) “Information Privacy in a Globally Networked Society: Implications for IS Research”, *Communications of the Association for Information Systems* (12) Article 22, pp. 341–365.

DeMarco, D.A. (2006) “Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six Packs”, *Texas Law Review* (84)4, pp. 1013–1064.

*Dinev, T. et al. (2006) “Privacy Calculus Model in E-Commerce—A Study of Italy and the United States”, *European Journal of Information Systems* (15)4, pp. 389–402.

*Dinev, T. and P. Hart (2004) “Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model”, *Behavior and Information Technology* (23)6, pp. 413–422.

*Dinev, T. and P. Hart (2005) “Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact”, *International Journal of Electronic Commerce* (10)2, pp. 7–29.

*Dinev, T. and P. Hart (2006) “An Extended Privacy Calculus Model for E-Commerce Transactions”, *Information Systems Research* (17)1, pp. 61–80.

*Dinev, T., P. Hart, and M.R. Mullen (2008) “Internet Privacy Concerns and Beliefs About Government Surveillance—An Empirical Investigation”, *Journal of Strategic Information Systems* (17)3, pp. 214–233.

Dinev, T. and Q. Hu (2007) “The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies”, *Journal of the Association for Information Systems* (8)7, pp. 386–408.

Dourish, P. and K. Anderson (2006) “Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena”, *Human–Computer Interaction* (21)3, pp. 319–342.

*Eastlick, M.A., S.L. Lotz, and P. Warrington (2006) “Understanding Online B-to-C Relationship: An Investigated Model of Privacy Concerns, Trust, and Commitment”, *Journal of Business Research* (59)8, pp. 877–886.

*Faja, S. and S. Trimi (2006) “Influence of the Web Vendor’s Interventions on Privacy-Related Behaviors in E-Commerce”, *Communications of the Association for Information Systems* (17) Article 27, pp. 593–634.

Fenigstein, A. and P.A. Vanable (1992) “Paranoia and Self-Consciousness”, *Journal of Personality and Social Psychology* (62)1, pp. 129–138.

*Fogel, J. and E. Nehmad (2009) “Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns”, *Computers in Human Behavior* (25)1, pp. 153–160.

*Frye, N.E. and M.M. Dornisch (2010) “When Is Trust Not Enough? The Role of Perceived Privacy of Communication Tools in Comfort with Self-Disclosure”, *Computers in Human Behavior* (26)5, pp. 1120–1127.

Garfinkel, R., R. Gopal, and S. Thompson (2007) “Releasing Individually Identifiable Microdata with Privacy Protection Against Stochastic Threat: An Application to Health Information”, *Information Systems Research* (18)1, pp. 23–41.

Greenaway, K.E. and Y.E. Chan (2005) “Theoretical Explanations for Firms' Information Privacy Behaviors”, *Journal* *of the Association for Information Systems* (6)6, pp. 171–189.

Gross, D. (2010) "The 10 Biggest Tech 'Fails' of 2010", http://www.cnn.com/2010/TECH/innovation/12/28/tech.fails.year/ (current Jan. 14, 2011).

Hann, I. et al. (2007) "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach", *Journal of Management Information Systems* (24)2, pp.13–42.

Henderson, S.C. and C.A. Snyber (1999) "Personal Information Privacy: Implications for MIS Managers", *Information and Management* (36)4, pp. 213–220.

Hofstede, G. (1991) *Cultures and Organizations: Software of the Mind*, New York, NY: McGraw-Hill.

Hossain, M.M. and V.R. Prybutok (2008) "Consumer Acceptance of RFID Technology: An Exploratory Study", *IEEE Transactions on Engineering Management* (55)2, pp. 316–328.

*Hoy, M.G. and G. Milne (2010) "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users", *Journal of Interactive Advertising* (10)2, pp. 28–45.

Hunter, J.E. and F.L. Schmidt (2004) *Methods of Meta-Analysis: Correcting Error and Bias in Research Findings, 2nd edition,* Thousand Oaks, CA: Sage Publications, Inc.

*Hui, K.L., H.H. Teo, and S.Y.T. Lee (2007) "The Value of Privacy Assurance: An Exploratory Field Experiment", *MIS Quarterly* (31)1, pp. 19–33.

Igbaria, M. and J. Ilvari (1995) "The Effects of Self-Efficacy on Computer Usage", *Omega, The International Journal of Management Science* (23)6, pp. 587–605.

*Janda, S. (2008) "Does Gender Moderate the Effect of Online Concerns on Purchase Likelihood?" *Journal of Internet Commerce* (7)3, pp. 339–358.

*Janda, S. and L.L. Fair (2004) "Exploring Consumer Concerns Related to the Internet", *Journal of Internet Commerce* (3)1, pp. 1–21.

Jessor, R. and S. Jessor (1977) *Problem Behavior and Psychosocial Development: A Longitudinal Study of Youth*, New York, NY: Academic Press.

*Ji, P. and P.S. Lieber (2010) "Am I Safe? Exploring Relationships Between Primary Territories and Online Privacy", *Journal of Internet Commerce* (9)1, pp. 3–22.

*Joinson, A.N. et al. (2010) "Privacy, Trust, and Self-Disclosure Online", *Human–Computer Interaction* (25)1, pp. 1–24.

Jourdan, Z., R.K., Rainer, and T.E. Marshall (2008) "Business Intelligence: An Analysis of the Literature", *Information Systems Management* (25)2, pp. 121–131.

*Junglas, I.A., N.A. Johnson, and C. Spitzmuller (2008) "Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Service", *European Journal of Information Systems* (17)4, pp. 387–402.

Kassarjian, H.H. (1977) "Content Analysis in Consumer Research", *Journal of Consumer Research* (4)1, pp. 8–18.

*Kim, D.J. (2008) "Self-Perception-Based versus Transference-Based Trust Determinants in Computer-Mediated Transactions: A Cross-Cultural Comparison Study", *Journal of Management Information Systems* (24)4, pp. 13–45.

*Kim, D.J., D.L. Ferrin, and R.H. Raghav (2008a) "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents", *Decision Support Systems* (44)2, pp. 544–564.

*Kim, D.J., C. Steinfield, and Y. Lai (2008b) "Revisiting the Role of Web Assurance Seals in Business-to-Consumer Electronic Commerce", *Decision Support Systems* (44)4, pp. 1000–1015.

Koh, C.E. (2003) "IS Journal Review Process: A Survey on IS Research Practice and Journal Review Issues", *Information and Management* (40)8, pp. 743–756.

*Korzaan, M.L. and K.T. Boswell (2008) "The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions", *Journal of Computer Information Systems* (48)4, pp. 15–24.

*Krohn, F., X. Luo, and M.K. Hsu (2002) "Information Privacy and Online Behaviors", *Journal of Internet Commerce* (1)4, pp. 55–69.

*Kumar, N., K. Mohan, and R. Holowczak (2008) "Locking the Door but Leaving the Computer Vulnerable: Factors

Inhibiting Home Users' Adoption of Software Firewalls", *Decision Support Systems* (46)1, pp. 254–264.

*Lai, Y.L. and K.L. Hui (2004) "Opting-In or Opting-Out on the Internet: Does It Really Matter?" *Proceedings of the 25th International Conference on Information Systems*, Paper 63, pp. 781–792.

*Laric, M.V., D.A. Pitta and L.P. Katsanis (2009) "Consumer Concerns for Healthcare Information Privacy: A Comparison of U.S. and Canadian Perspectives", *Research in Healthcare Financial Management* (12)1, pp. 93–111.

*Lee, C.H. and D.A. Cranage (In press) "Personalisation-Privacy Paradox: The Effects of Personalisation and Privacy Assurance on Customer Responses to Travel Web Sites", *Tourism Management*.

Lee, S.M., T. Hwang, and J. Kim (2007) "An Analysis of Diversity in Electronic Commerce Research", *International Journal of Electronic Commerce* (12)1, pp. 31–67.

Li, X.B. and S. Sarkar (2006) "Privacy Protection in Data Mining: A Perturbation Approach for Categorical Data", *Information Systems Research* (17)3, pp. 254–270.

*Li, X., G. Rong, and J.B. Thatcher (2009) "Swift Trust in Web Vendors: The Role of Appearance and Functionality", *Journal of Organizational and End User Computing* (21)1, pp. 88–108.

Li, H., R. Sarathy, and H. Xu (2010) "Understanding Situational Online Information Disclosure as a Privacy Calculus", *Journal of Computer Information Systems* (51)1, pp. 62–71.

*Lian, J.W. and T.M. Lin (2008) "Effects of Consumer Characteristics on Their Acceptance of Online Shopping: Comparisons Among Different Product Types", *Computers in Human Behavior* (24)1, pp. 48–65.

*Liu, C., J.T. Marchewka, and C. Ku (2004) "American and Taiwanese Perceptions Concerning Privacy, Trust, and Behavioral Intentions in Electronic Commerce", *Journal of Global Information Management* (12)1, pp. 18–40.

*Liu, C. et al. (2005) "Beyond Concern—A Privacy–Trust-Behavioral Intention Model of Electronic Commerce", *Information and Management* (42)2, pp. 289–304.

*Luo, X. and M. Seyedian (2003) "Contextual Marketing and Customer-Orientation Strategy for E-Commerce: An Empirical Analysis", *International Journal of Electronic Commerce* (8)2, pp. 95–118.

Lwicki, R.J., D.J. McAllister, and R.J. Bies (1998) "Trust and Distrust: New Relationships and Realities", *Academy of Management Review* (23)3, pp. 438–458.

*Lwin, M., J. Wirtz, and J.D. Williams (2007) "Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective", *Journal of the Academy of Marketing Science* (35)4, pp. 572–585.

*Malhotra, N.K., S.S. Kim, and J. Agarwal (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", *Information Systems Research* (15)4, pp. 336–355.

MacMillan, D. (2010) "Facebook's Washington Problem", *Businessweek*, May 17–May 23, pp. 33–34.

*McCole, P., E. Ramsey, and J. Williams (2010) "Trust Considerations on Attitudes Towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns", *Journal of Business Research* (63)9–10, pp. 1018–1024.

McCrae, R.R. and P. Costa (1999) "A Five Factor Theory of Personality" in Pervin, L. (ed.) *Handbook of Personality: Theory and Research,* New York, NY: Guilford, pp 139–153.

McKnight, D.H. and N.L. Chervany (2002) "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology", *International Journal of Electronic Commerce* (6)2, pp. 35–59.

Meinert, D.B. et al. (2006) "Privacy Policy Statements and Consumer Willingness to Provide Personal Information", *Journal of Electronic Commerce in Organizations* (4)1, pp. 1–17.

*Milberg, S.J., H.J. Smith, and S.J. Burke (2000) "Information Privacy: Corporate Management and National Regulation", *Organization Science* (11)1, pp. 35–57.

*Nam, C. et al. (2006) "Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online", *Advances in Consumer Research* (33)1, pp. 212–217.

Neuendorf, K.A. (2002) *The Content Analysis Guidebook*, Thousand Oaks, CA: Sage Publications, Inc.

Ngai, E.W.T. and F.K.T. Wat (2002) "A Literature Review and Classification of Electronic Commerce Research", *Information and Management* (39)5, pp. 415–429.

*Okazaki, S., H. Li, and M. Hirose (2009) "Consumer Privacy Concerns and Preference for Degree of Regulatory Control", *Journal of Advertising* (38)4, pp. 63–77.

Paine, C. et al. (2007) “Internet Users' Perceptions of ‘Privacy Concerns’ and ‘Privacy Actions’”, *International Journal of Human–Computer Studies* (65)6, pp. 526–536.

Parasuraman, S. and M. Igbaria (1990) “An Examination of Gender Differences in the Determinants of Computer Anxiety and Attitudes Toward Microcomputers Among Managers”, *International Journal of Man–Machine Studies* (2)3, pp. 327–340.

Pavlou, P.A. (2003) “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model”, *International Journal of Electronic Commerce* (7)3, pp. 69–103.

*Pavlou, P., H. Liang, and Y. Xue (2007) “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principle–Agent Perspective”, *MIS Quarterly* (31)1, pp. 105–136.

Peltier, J.W., G.R. Milne, and J.E. Phelps (2009) “Information Privacy Research: Framework for Integrating Multiple Publics, Information Channels, and Responses”, *Journal of Interactive Marketing* (23)2, pp. 191–205.

*Phelps, J.E., G. D'Souza, and G.J. Nowak (2001) “Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation”, *Journal of Interactive Marketing* (15)4, pp. 2–17.

Potter, W.J. and D. Levine-Donnerstein (1999) “Rethinking Validity and Reliability in Content Analysis”, *Journal of Applied Communication Research* (27)3, pp. 258–284.

*Premazzi, K. et al. (2010) “Customer Information Sharing with E-Vendors: The Roles of Incentives and Trust”, *International Journal of Electronic Commerce* (14)3, pp. 63–91.

Prince, K. and M. Barrett (2005) “Privacy Implications of Technology Innovation Processes”, *Proceedings of the 26th International Conference on Information Systems,* Paper 35, pp. 423–433.

*Rensel, A.D., J.M. Abbas, and H.R. Rao (2006) “Private Transactions in Public Places: An Exploration of the Impact of the Computer Environment on Public Transactional Web Site Use”, *Journal of the Association for Information Systems* (7)1, pp. 19–51.

*Rifon, N.J., R. LaRose, and S.M. Choi (2005) “Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures”, *Journal of Consumer Affairs* (39)2, pp. 339–362.

*Roca, J.C., J.J. Garcia, and J. de la Vega (2009) “The Importance of Perceived Trust, Security and Privacy in Online Trading Systems”, *Information Management & Computer Security* (17)2, pp. 96–113.

*Rohm, A.J. and G.R. Milne (2004) “Just What the Doctor Ordered—The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern”, *Journal of Business Research* (57)9, pp. 1000–1011.

Rosenberg, M. et al. (1995) “Global Self-Esteem and Specific Self-Esteem: Different Concepts, Different Outcomes”, *American Sociological Review* (60)1, pp. 141–156.

Saeed, K.A., Y. Hwang, and M.Y. Yi (2003) “Toward an Integrative Framework for Online Consumer Behavior Research: A Meta-Analysis Approach”, *Journal of End User Computing* (15)4, pp. 1–26.

Schwaig, K.S., G.C. Kane, and V.C. Storey (2006) “Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures?” *Information and Management* (43)7, pp. 805–820.

Schwarz, A. et al. (2007) “Understanding Frameworks and Reviews: A Commentary to Assist Us in Moving Our Field Forward by Analyzing Our Past”, *The DATA BASE for Advances in Information Systems* (38)3, pp. 29–50.

*Sheehan, K.B. (1999). “An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors”, *Journal of Interactive Marketing* (13)4, pp. 24–38.

*Sheehan, K.B. and M.G. Hoy (1999) “Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns”, *Journal of Advertising* (28)3, pp. 37–51.

*Sheng, H., F.F. Nah, and K. Siau (2008) “An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personal Personalization and Privacy Concerns”, *Journal of the Association for Information Systems* (9)6, pp. 344–376.

*Shin, D.H. (2010) “The Effects of Trust, Security and Privacy in Social Networking: A Security-Based Approach to Understand the Pattern of Adoption”, *Interacting with Computers* (22)5, pp. 428–438.

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

Smyth, B. (2007) “Adaptive Information Access: Personalization and Privacy”, *International Journal of Pattern Recognition & Artificial Intelligence* (21)2, pp. 183–205.

*Son, J. and S.S. Kim (2008) “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model”, *MIS Quarterly* (32)3, pp. 503–529.

Stanton, J.M. and K. Stam (2003) “Information Technology, Privacy, and Power Within Organizations: A Merger of Boundary Theory and Social Exchange Perspectives”, *Surveillance and Society* (1)2, pp. 152–190.

*Stewart, K.A. and A.H. Segars (2002) “An Empirical Examination of the Concern for Information Privacy Instrument”, *Information Systems Research* (13)1, pp. 36–49.

Straub, D. et al. (2002) “Toward a Theory-Based Measurement of Culture”, *Journal of Global Information Management* (10)1, pp. 13–23.

*Stutzman, F., R. Capra, and J. Thompson (2011) “Factors Mediating Disclosure in Social Network Sites”, *Computers in Human Behavior* (27)1, pp. 590–598.

Tam, E., K. Hui, and B. Tan (2002) “What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses”, *Proceedings of the 23rd International Conference on Information Systems*, Paper 2, pp. 11–21.

Thatcher, J.B. and P.L. Perrewe (2002) “An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy”, *MIS Quarterly* (26)4, pp. 381–396.

*Tsarenko, Y. and D.R. Tojib (2009) “Examining Customer Privacy Concerns in Dealings with Financial Institutions”, *Journal of Consumer Marketing* (26)7, pp. 468–476.

*Van Slyke, C. et al. (2006) “Concerns for Information Privacy and Online Consumer Purchasing”, *Journal of the Association for Information Systems* (7)6, pp. 415–444.

Wang, H., M.K.O. Lee, and C. Wang (1998) “Consumer Privacy Concerns about Internet Marketing”, *Communications of the ACM* (41)3, pp. 63–70.

*Ward, S., K. Bridges, and B. Chitty (2005) “Do Incentives Matter? An Examination of On-Line Privacy Concerns and Willingness to Provide Personal and Financial Information”, *Journal of Marketing Communications* (11)1, pp. 21–40.

Webster, J. (1998) “Desktop Videoconferencing: Experiences of Complete Users, Wary Users, and Non-Users”, *MIS Quarterly* (22)3, pp. 257–286.

*Wei, R., X. Hao, and J. Pan (2010) “Examining User Behavioral Response to SMS Ads: Implications for the Evolution of the Mobile Phone as a Bona-Fide Medium”, *Telematics and Informatics* (27)1, pp. 32–41.

*Wirtz, J., M.O. Lwin, and J.D. Williams (2007) “Causes and Consequences of Consumer Online Privacy Concern”, *International Journal of Service Industry Management* (18)4, pp. 326–348.

Wood, W. (2000) “Attitude Change: Persuasion and Social Influence”, *Annual Review of Psychology* (51)1, pp. 539–570.

Woodman, R.W. et al. (1982) “A Survey of Employee Perceptions of Information Privacy in Organizations”, *Academy of Management Journal* (25)3, pp. 647–663.

*Xu, H. (2007) “The Effects of Self-Construal and Perceived Control on Privacy Concerns”, *Proceedings of the 28th International Conference on Information Systems*, Paper 125, pp. 1–14.

*Xu, H. et al. (2008) “Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View”, *Proceedings of the 29th International Conference on Information Systems*, Paper 6, pp. 1–16.

*Xu, H. and H.H. Teo (2004) “Alleviating Consumers’ Privacy Concerns in Location-Based Services: A Psychological Control Perspective”, *Proceedings of the 25th International Conference on Information Systems*, Paper 64, pp. 793–806.

Xu, H., H.H. Teo, and B. Tan (2005) “Predicting the Adoption of Location-Based Service: The Role of Trust and Perceived Privacy Risk”, *Proceedings of the 26th International Conference on Information Systems,* Paper 71, pp. 897–910.

*Yang, S. and K. Wang (2009) “The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioral Intention”, *The DATA BASE for Advances in Information Systems* (40)1, pp. 38–51.

*Yao, Y. and L. Murphy (2007) “Remote Electronic Voting Systems: An Exploration of Voters’ Perceptions and Intention to Use”, *European Journal of Information Systems* (16)2, pp. 106–120.

*Yao, M.Z., R.E. Rice, and K. Wallis (2007) “Predicting User Concerns about Online Privacy”, *Journal of the American Society for Information Science and Technology* (58)5, pp. 710–722.

*Yao, M.Z. and J. Zhang (2008) “Predicting User Concerns About Online Privacy in Hong Kong”, *CyberPsychology and Behavior* (11)6, pp. 779–781.

*Youn, S. (2008) “Parental Influence and Teens' Attitude Toward Online Privacy Protection”, *Journal of Consumer Affairs* (42)3, pp. 362–388.

*Youn, S. (2009) “Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents”, *Journal of Consumer Affairs* (43)3, pp. 389–418.

*Yousafzai, S., J. Pallister, and G. Foxall (2009) “Multi-Dimensional Role of Trust in Internet Banking Adoption”, *Service Industries Journal* (29)5, pp. 591–605.

*Zhang, Y., J.Q. Chen, and K.W. Wen (2002) “Characteristics of Internet Users and Their Privacy Concerns—A Comparative Study Between China and the United States”, *Journal of Internet Commerce* (1)2, pp. 1–16.

*Zimmer, J.C. et al. (2010) “Knowing your Customers: Using a Reciprocal Relationship to Enhance Voluntary Information Disclosure”, *Decision Support Systems* (48)2, pp. 395–406.

*Zviran, M. (2008) “User’s Perspectives on Privacy in Web-Based Applications”, *Journal of Computer Information Systems* (48)4, pp. 97–105.

APPENDIX A: LITERATURE REVIEWED IN THE STUDY

Table A-1: Literature Reviewed in the Study

Literature	Research objective	Privacy construct and measurement	Research method	Subjects and sample size (N)	Data analysis method
Andrade et al. [2002]	Examine approaches to encouraging self-disclosure of personal information on the Internet	Concerns for self-disclosure of information; New scale with three dimensions: concerns for identification information, sensitive information, and preferences and habits	Experiment	Undergraduate students in an U.S. university; N = 114	Analysis of variance (ANOVA)
Angst and Agarwal [2009]	Test the changes of individuals’ attitudes and opt-in intentions in the adoption of electronic health records	Concerns for Information Privacy (CFIP); 2nd-order construct adapted from Smith et al. [1996]	Experiment	Individuals attending a health conference; N = 366	Structural equation modeling (SEM)
Ashley et al. [in press]	Study the factors that affect customer engagement in relationship marketing efforts	Privacy concerns; New scale	Survey	Households in the U.S.; N = 251	SEM
Awad and Krishnan [2006]	Examine the relationship between information transparency and willingness to be profiled online	Privacy concerns; 2 items adapted from past research	Survey	Internet users participating in product evaluations; N = 523	SEM
Bansal et al. [2008]	Examine how the quality of privacy policy statements and privacy assurance cues contribute to increased online trust	Privacy concerns; 2nd-order construct adapted from Smith et al. [1996]	Experiment	Students from an U.S. university; N = 674	SEM
Bansal et al. [2010]	Study the factors that affect an individual’s intention to disclose health information online	Health information privacy concerns; 3 items adapted from past research	Experiment	Students from an U.S. university; N = 367	SEM
Bellman et al. [2004]	Examine international differences in information privacy concerns and the impact of three antecedents	CFIP; 2nd-order construct adapted from Smith et al. [1996]	Survey	Internet users from 38 countries; N = 534	Multivariate analysis of covariance (MANCOVA)
Buchanan et al. [2007]	Develop short Internet-administered scales measuring online privacy concern and behaviors (General Caution and Technical Protection)	Online privacy concerns; New scale with 16 unidimensional items	Survey	Students from an university in the U.K.; N1 = 515, N2 = 69, and N3 = 1,122	Factor analysis, correlations

Table A-1: Literature Reviewed in the Study - Continued

Casalo et al. [2007]	Analyze the influence of several factors on consumer trust in online banking	Perceived website privacy; 7 items adapted from past research	Survey	Spanish-speaking Internet users; N = 142	SEM
Cases et al. [2010]	Study the impact of several factors on email campaign effectiveness	Perceived privacy concerns; 3 items measuring perceived privacy	Survey	Shoppers of a Web company; N = 330	SEM
Cazier et al. [2008]	Study the factors that influence customers' intention to use radio frequency identification technologies (RFID)	Perceived privacy risk likelihood and perceived privacy risk harm; New scales	Survey	U.S. residents; N = 320	SEM
Chen et al. [2001b]	Investigate the relationship between consumer characteristics and online information privacy concerns	Information privacy concerns; 3 dimensions adapted from Smith et al. [1996]	Survey	Combination of students, faculty, and researchers in the U.S.; N = 340	Correlation
Chen et al. [2009]	Study the Privacy Concerns About Peer's Disclosure of one's information (PCAPD)	PCAPD; 7 items adapted from past research	Experiment	Students from a university; N = 209	Analysis of Covariance (ANCOVA) and regression
Chen and Rea [2004]	Study the factors that influence the use of privacy control techniques to protect personal information online	Privacy concerns; Two-dimensions adapted from Smith et al. [1996]	Survey	Undergraduate students; N = 102	Multiple regression
Cheung and Liao [2003]	Examine the supply-side hurdles in B2C e-commerce in Hong Kong	Privacy concerns; New scale	Survey	Hong Kong residents; N = 138	Multivariate regression
Chiu et al. [2009]	Understand e-shoppers' repurchase intentions	Privacy; 3 items adapted from past research	Survey	E-shoppers in Taiwan; N = 360	SEM
Cocosila et al. [2009]	Study the early investigation of new IT acceptance	Perceived privacy risks; 3 items adapted from past research	Experiment	Participants recruited from a university website; N = 303	SEM
Culnan and Armstrong [1999]	Study the impact of procedural fairness on the relationship between privacy concerns and customers' willingness to be profiled	Privacy concerns; New scale	Survey	U.S. households; N = 1,000	Discriminant analysis
Dai and Palvia [2009]	A comparative examination of factors affecting mobile commerce adoption	Privacy perception; New scale	Survey	A convenient sample of m-commerce users in China (N = 106) and students in the U.S. (N = 84)	SEM
Dinev et al. [2006]	Examines cross-cultural differences in beliefs related to e-commerce use for Italy and the United States	Privacy concerns; 4-item uni-dimensional construct adapted from Dinev and Hart, 2004, 2006	Survey	Individuals from Italy (N = 889) and the U.S. (N = 422)	SEM
Dinev and Hart [2004]	Develop an instrument to measure Internet privacy concerns and test the impact of two antecedents	Perceived privacy concerns; New scale with 2 dimensions: finding and abuse	Survey	Students and employees from universities and companies in the U.S.; N = 369	Regression
Dinev and Hart [2005]	Study the antecedents of privacy concerns and the intention to conduct online transactions	Internet privacy concerns; Information abuse dimension from Dinev and Hart [2004]	Survey	A combination of residents, teachers, students, and employees; N = 422	SEM

Table A-1: Literature Reviewed in the Study - Continued

Dinev and Hart [2006]	Study the impact of privacy risk beliefs on information privacy and the intention to provide personal information for online transactions	Internet privacy concerns; 4 items adapted from Smith et al. [1996] and Culnan and Armstrong [1999]	Survey	A combination of residents, teachers, students, and employees; N = 369	SEM
Dinev et al. [2008]	Test the relationship between Internet privacy concerns and the consequences under government surveillance	Internet privacy concerns; Two dimensions adapted from Dinev and Hart [2004, 2006]	Survey	A broad sample of individuals from various industries in the U.S.; N = 422	SEM
Eastlick et al. [2006]	Test the applicability of a traditional B2B relationship marketing framework to the B2C channel	Privacy concerns; 4 items adapted from focus group results and past research	Survey	U.S. households; N = 477	SEM
Faja and Trimi [2006]	Test the impact of a website's privacy interventions on users' perceptions and intentions during the initial interaction	General CFIP: adapted from Smith et al. [1996] and developed by authors; Perceived information privacy: adapted from past research and developed by authors	Experiment	Students from 2 U.S. universities; N = 210	ANCOVA and multiple regressions
Fogel and Nehmad [2009]	Study the associations between social networking user attributes and privacy concerns, risk taking and trust	Privacy concerns 3 items adapted from Dinev and Hart [2004]	Survey	College students in the U.S.; N = 205	ANOVA
Frye and Dornisch [2010]	Study the impact of topic intimacy and perceived privacy on the disclosure of information via instant messaging	Perceived privacy of a medium; Single item	Survey	Individuals from multiple nations; N = 214	Correlation and regression
Hoy and Milne [2010]	Examine gender differences in young adults' privacy beliefs, reactions to behavioral advertising and information sharing and privacy protection on social networks	Privacy concerns; Single item	Survey	Facebook.com users; N = 589	T-test
Hui et al. [2007]	Study the impact of privacy statements and privacy seals on information disclosure by individuals	Privacy concerns; Adapted from Smith et al. [1996]	Survey	Business students in Singapore; N = 109	Logistic regression
Janda [2008]	Study the impact of four consumer online concerns (privacy, security, etc.) on the likelihood of making online purchases, and the moderating role of gender	Privacy concerns; New scale	Survey	Nonstudent Internet users; N = 404	SEM
Janda and Fair [2004]	Identify eleven potential concerns people may have about the Internet, including privacy, fraud, etc.	Privacy concerns; New scale	Survey	Non-student Internet users; N = 440	T-test
Ji and Lieber [2010]	Study the link between personal identifiable information (PII) disclosure and privacy concerns	Worry about information disclosure online; Single item	Survey	Adult Internet users; N = 1,623	Logistic regression
Joinson et al. [2010]	Study the link between online privacy concerns and actual behavior	Privacy dispositions and perceived privacy; Adapted from past research	Survey and experiment	Students and Internet users from multiple nations; N1 = 759, N2 = 181	Correlation, ANOVA, and linear regression
Junglas et al. [2008]	Study the factors that influence CFIP	CFIP; 2nd-order construct adapted from Smith et al. [1996]	Survey	Undergraduate and graduate business students; N = 378	SEM

Table A-1: Literature Reviewed in the Study - Continued

Kim [2008]	Examine the impact of culture on trust determinants in computer-mediated transactions	Privacy concerns; New scale	Survey	Students from universities in the U.S. (N = 246) and South Korea (N = 199)	SEM
Kim et al. [2008a]	Test the impact of trust and risk in consumers' electronic commerce purchasing decisions	Perceived privacy protection; New scale	Quasi-experiment	Undergraduate students; N = 468	SEM
Kim et al. [2008b]	Examine the effects of an educational intervention on consumer's knowledge of security and privacy	Privacy concerns; 4 items adapted from past research	Quasi-experiment	Undergraduate students in an U.S. university; N = 125	t-tests, SEM
Korzaan and Boswell [2008]	Test the impact of personality traits on CFIP	CFIP; 2nd-order construct adapted from Smith et al. [1996]	Survey	Undergraduate students; N = 230	SEM
Krohn et al. [2002]	Study the potential influences of privacy concerns on consumers' attitudes toward websites and their satisfaction, etc.	Privacy concerns; Adapted from past research	Survey	College students from the U.S.; N = 219	Multiple regression
Kumar et al. [2008]	Investigate the factors that affect the use of security protection strategies by home computer users	CFIP; 2nd-order construct adapted from Stewart and Segars [2002]	Survey	Students from a public university in the U.S.; N = 120	SEM
Lai and Hui [2004]	Explain the differences in consumer participations in opt-in and opt-out configurations	Privacy concerns; 2nd-order construct adapted from Smith et al. [1996]	Experiment	Undergraduate and postgraduate students; N = 32	t-tests
Laric et al. [2009]	Study the impact of a number of factors on healthcare privacy concerns	Concerns for healthcare; information privacy New scale	Survey	MBA students from the U.S. and Canada; N = 225	ANOVA
Lee and Cranage [in press]	Study the effects of personalization and privacy assurance on customer responses to travel websites	Privacy concerns; Adapted from past research	Experiment	Undergraduate students in the U.S.; N = 120	ANOVA and regression
Li et al. [2009]	Examine how Web vendors may foster swift trust among customers	Perceived privacy; Adapted from past research	Experiment	College students; N = 224	SEM
Lian and Lin [2008]	Examine the effects of consumer characteristics (such as privacy concerns) on online shopping acceptance in the context of different products and services	Privacy concerns; Adapted from Smith et al. [1996]	Survey	Undergraduate students in Taiwan; N = 216	Regression
Liu et al. [2004]	Compare American and Taiwanese perceptions of online privacy and the impact on trust on websites	Perceived privacy; New scale	Experiment	Undergraduate and graduate students in the U.S. and Taiwan; N = 436	Correlation
Liu et al. [2005]	Study how perceived privacy relates to the behavioral intention to make an online transaction.	Perceived privacy; New scale	Experiment	Undergraduate and graduate students in the U.S.; N = 212	SEM
Luo and Seyedian [2003]	Test the moderating effects in contextual marketing and customer-oriented strategies	Privacy concerns; 5 items adapted from literature	Survey	Internet users in the U.S.; N = 180	Regression

Table A-1: Literature Reviewed in the Study - Continued

Lwin et al. [2007]	Test the mediating effect of privacy concern on the link between business policy and regulatory perceptions, and users' protective online responses	Online privacy concerns; Adapted from past research	Experiment	Adult Internet users from multiple nations; N1 = 180, N2 = 627	ANOVA
Malhotra et al. [2004]	Develop a new scale to measure Internet Users' Information Privacy Concerns (IUIPC)	IUIPC; New scale	Experiment	Household Internet users; N = 449	SEM
McCole et al. [2010]	Test the moderating effect of privacy and security concerns on the impact of trust on online purchasing attitudes	Privacy and security concerns; Adapted from past research	Survey	Employees in an New Zealand universities; N = 383	Hierarchical regression, ANOVA
Milberg et al. [2000]	Test the impact of regulatory approaches on information privacy, corporate management of personal data and consumer reactions	CFIP; 2nd-order construct adapted from Smith et al. [1996]	Survey	Members of a multi-national association; N = 595	SEM
Nam et al. [2006]	Study the factors that influence consumers' privacy concerns and their willingness to provide marketing-related personal information online	Privacy concerns; Adapted from past research	Survey	Internet users in Korea; N = 323	SEM
Okazaki et al. [2009]	Explores the consequences of consumers' privacy concerns in the mobile advertising context in Japan	Privacy concerns; Adapted from Malhotra et al. [2004]	Quasi-experiment	Japanese mobile users; N = 510	SEM
Pavlou et al. [2007]	Study the nature of online uncertainty and the mitigation approaches	Information privacy concerns; 6 items adapted from Smith et al. [1996] and other research	Survey	Visitors to an online bookstore (N1 = 268), and visitors to an prescription filling website (N2 = 253)	SEM
Phelps et al. [2001]	Examine the interrelationships among antecedents and consequences of privacy concerns	Privacy concerns; Single item	Survey	U.S. households; N = 556	Regression
Premazzi et al. [2010]	Study the roles of incentives and trust in customer information sharing with e-vendors	Privacy concerns; Adapted from Smith et al. [1996]	Experiment	Firm employees in Italy; N = 178	ANOVA, ANCOVA, and regression
Rensel et al. [2006]	Test people's willingness to use publicly-available computers for e-commerce transactions	Task privacy; Adapted from past research	Survey	Public library patrons in the U.S.; N = 137	SEM
Rifon et al. [2005]	Study the effects of Web privacy seals on trust and personal disclosures and the impact of several moderators such as privacy concerns	Privacy concerns; New scale	Experiment	Undergraduate students in the U.S.; N = 210	ANOVA
Roca et al. [2009]	Investigate how e-investors are influenced by perceived trust, security, privacy and other constructs	Perceived privacy; 4 items adapted from past research	Survey	Undergraduate students in Spain; N = 103	SEM
Rohm and Milne [2004]	Examine consumer concern regarding the collection and use of personal medical information	Privacy concerns regarding specific types of information; New scale	Survey	U.S. households; N = 1,508	z-test

Table A-1: Literature Reviewed in the Study - Continued

Sheehan [1999]	Investigate gender difference in online privacy concerns	Privacy concerns; New scale	Survey	U.S. households; N = 889	t-test
Sheehan and Hoy [1999]	Study online consumers' response to privacy concerns	Privacy concerns; New scale	Survey	Internet users in the U.S.; N = 889	Correlation
Sheng et al. [2008]	Examines how personalization and context can impact customers' privacy concerns and the intention to adopt ubiquitous commerce	Privacy concerns; 4 items adapted from Smith et al. [1996] and Dinev and Hart [2004]	Experiment	University students in the U.S.; N = 100	Regression
Shin [2010]	Test the effects of trust, security and privacy in social networking	Perceived privacy; Adapted from past research	Survey	College students in the U.S.; N = 323	SEM
Smith et al. [1996]	Develop an instrument to measure CFIP	CFIP; New, 4-dimensional scale	Survey	Multiple samples: business graduate students (N = 77), undergraduate students (N = 59; N = 87; and N = 83) in the U.S.	Regression and correlation
Son and Kim [2008]	Develop a taxonomy of information privacy-protective responses and to test the impact of some antecedents	Information privacy concerns; 4 items adapted from Dinev and Hart [2006]	Survey	Panel members of a market research firm; N = 523	SEM
Stewart and Segars [2002]	Examine the factor structure of the CFIP instrument by Smith et al. [1996]	CFIP; 2nd-order construct based on Smith et al. [1996]	Survey	U.S. consumers (mall-shoppers); N = 355	SEM
Stutzman et al. [2011]	Explore how privacy settings and privacy policy consumption affect the relationship between privacy attitudes and disclosure behaviors in Facebook.com	Privacy attitude; Adapted from past research	Survey	University students in the U.S.; N = 122	Logistic regression
Tsarenko and Tojib [2009]	Examine the driving factors of privacy concern	Privacy concerns; Adapted from Smith et al. [1996]	Survey	Australian consumers; N = 456	Hierarchical regression
Van Slyke et al. [2006]	Assess the impact of consumers' concerns for information privacy on their willingness to engage in online transactions	CFIP; 2nd-order formative construct adapted from Smith et al. [1996] and Stewart and Segars [2002]	Survey	Visitors to Amazon.com (N = 713) and to Half.com (N = 287) from the U.S.	SEM
Ward et al. [2005]	Examine online privacy concerns and willingness to provide financial and personal information	Privacy concerns; Single item	Experiment	University students in Australia; N = 315	ANCOVA
Wei et al. [2010]	Study the factors that influence users' behavioral responses to short message service (SMS) ads	Privacy concerns; New scale	Survey	College students in Singapore; N = 407	Hierarchical regression
Wirtz et al. [2007]	Study the causes and consequences of online privacy concerns	Privacy concerns; Adapted from past research	Survey	Adult Internet users; N = 182	SEM
Xu [2007]	Examine the factors that alleviate privacy concerns in mobile computing	Privacy concerns; 4 items adapted from Smith et al. [1996]	Experiment	Mobile phone users in Singapore; N = 179	SEM
Xu and Teo [2004]	Examine the factors that alleviate privacy concerns in mobile computing	Privacy concerns; 7 items adapted from Dinev and Hart [2004] and Smith et al. [1996]	Experiment	Undergraduate students in Singapore; N = 256	SEM

Table A-1: Literature Reviewed in the Study - Continued

Xu et al. [2008]	Examine the formation of individuals' privacy concerns	Privacy concerns; 5 items adapted from Smith et al. [1996]	Survey	Undergraduate and graduate students at three universities in the U.S.; N = 823	SEM
Yang and Wang [2009]	Test the impact of information sensitivity and compensation on privacy concern and behavioral intention	CFIP; 2nd-order construct adapted from Malhotra et al. [2004] and Smith et al. [1996]	Experiment	Students from 2 universities in China; N = 458	Multivariate regression and ANOVA
Yao et al. [2007]	Test the impact of a number of antecedents on information privacy concerns	Concerns about online privacy; 11 items adapted from Smith et al. [1996] were used to measure organizational privacy; these items, along with 9 additional items, were used to measure online privacy	Survey	Undergraduate students in an U.S. university; N = 413	SEM
Yao and Murphy [2007]	Explore voters' perceptions and intention to use remote electronic voting systems	Privacy; New scale	Survey	U.S. citizens; N = 453	SEM
Yao and Zhang [2008]	Study factors that predict users' online privacy concerns in Hong Kong	Privacy concerns; Adapted from Smith et al., 1996	Survey	Undergraduate students in Hong Kong; N = 332	SEM
Youn [2008]	Examine the impact of parental influence on teens' attitude toward privacy protection.	Teens' privacy concerns; Adapted from past research	Survey	Public high-school students in U.S.; N = 395	Regression
Youn [2009]	Study the determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents	Privacy concerns; Single item	Survey	Middle school students in the U.S.; N = 144	Regression
Yousafzai et al. [2009]	Develop and validate a multi-dimensional model of trust for Internet banking	Perceived privacy; Adapted from past research	Survey	Internet banking users from the U.K.; N = 441	SEM
Zhang et al. [2002]	Compares the privacy concerns of online consumers in China and the U.S. and identify major factors related to these concerns	Privacy concerns; New scale	Survey	Students, faculty and managerial professionals from the U.S. (N = 340) and China (N = 106)	t-test
Zimmer et al. [2010]	Examine the link between intent to disclose information and the actual disclosure	Information privacy concerns; 6 items adapted from Malhotra et al. [2004]	Experiment	Business management students in the U.S.; N = 236	Regression analysis
Zviran [2008]	Study factors that affect online privacy concerns and how these concerns could affect the users' online behavior	Privacy concerns; 5 dimensions adapted from past research	Survey	Graduates from an Israeli university; N = 217	Pearson correlation and ANOVA

APPENDIX B: ANTECEDENTS OF THE PRIVACY CONSTRUCT

Table B-1: Antecedents of the Privacy Construct

Literature	Privacy construct	Antecedents	Major findings
Andrade et al. [2002]	Concerns for self-disclosure of information	Reputation of a company; completeness of the privacy policy; offer of a reward; and the nature of the information inquired	The reputation of a company decreased self-disclosure concerns (F = 3.273, p < .08), the completeness of privacy policy also alleviates the concerns (F = 4.018; p < .05), but to the contrary the offer of a reward intensifies the concerns over disclosure (F = 3.477, p < .07). Sensitive information induces stronger concerns than identification information, which in turn induces stronger concerns than preferences and habits.
Bansal et al. [2010]	Health information privacy concerns	Perceived health information sensitivity, and previous online privacy invasion regarding health information	Both perceived health information sensitivity (β = .28, p < .001) and previous online privacy invasion (β = .17, p < .001) have a positive impact on health information privacy concerns
Bellman et al. [2004]	CFIP	Culture values, regulatory structure, and individual's Internet experience	Three culture dimensions—power distance, individualism, and uncertainty avoidance—each have an impact on privacy concerns; the impact is fully mediated by regulatory structure. The latter does not have a consistent impact on privacy concerns. Individual's Internet experience has a negative impact on CFIP (F = 2.12, p < .05).
Chen et al. [2001b]	Information privacy concerns	Age, income, education, online shopping experience	For individuals without online shopping experience, age has a positive relationship with the concern of misuse of credit cards (r = .23, p < .05). No other relationships are significant.
Chen et al. [2009]	Privacy concerns about peer's disclosure of one's information (PCAPD)	Social network overlap, decisional control, and information exclusivity	Decisional control (F = 4.303, p < 0.05) and information exclusivity (F = 33.923, p < 0.01) both have an impact on PCAPD; the impact of social network overlap on PCAPD was not supported.
Dinev et al. [2006]	Privacy concerns	Perceived risk	Perceived risk is positively associated with privacy concerns (Italy—β = .68, p < .01; U.S.—β = .36, p < .01).
Dinev and Hart [2004]	Perceived privacy concerns	Perceived vulnerability and perceived ability to control information	Perceived vulnerability is positively related to information privacy concerns (Finding-β = .39, p<.001; Abuse-β = .35, p < .001), but perceived ability to control information has no impact.
Dinev and Hart [2005]	Internet privacy concerns	Internet literacy and Social awareness	Internet literacy is negatively associated with privacy concerns (β = -.17, p < .01), and social awareness is positively associated with privacy concerns (β = .18, p < .01).
Dinev and Hart [2006]	Internet privacy concerns	Perceived Internet privacy risk	Perceived Internet privacy risk is positively associated with privacy concerns (β = -.33, p < .01).
Eastlick et al. [2006]	Privacy concerns	Reputation of an e-commerce website	E-commerce website reputation has a negative impact on privacy concerns (β = -.28, p < .05).
Faja and Trimi [2006]	General CFIP and Perceived information privacy	Web vendor privacy-related intervention	Vendor intervention has a positive impact on site-specific privacy perceptions (F = 4.383, p < .05).
Fogel and Nehmad [2009]	Privacy concerns	Having (or not) a social networking profile, gender,	Women have significantly greater concerns about information privacy than men (F = 6.25, p = .013); having a social networking profile or not does not have a strong relationship with privacy concerns.
Frye and Dornisch [2010]	Perceived privacy of a medium	Frequency of use of communication medium	Frequency of use has no significant association with perceived privacy of the medium
Hoy and Milne [2010]	Privacy concerns	Gender	Women are significantly more concerned than men about information privacy on Facebook (t = -4.12, p < .001)

Table B-1: Antecedents of the Privacy Construct - Continued

Janda and Fair [2004]	Privacy concerns	Gender, online purchase experience (buyers versus non-buyers), and age	Women are more concerns about privacy than men (t = 2.58, p < .01); no difference is observed between buyers and non-buyers; age is positively associated with privacy concerns (r = .23, p < .001)
Ji and Lieber [2010]	Worry about information disclosure online	Online disclosure of PII, age; education and gender are used as control variables	Online disclosure of PII (home address and video only) is significantly associated with worry (F = .018); the impact of age is mixed; education and gender have no impact on worry.
Joinson et al. [2010]	Privacy dispositions and perceived privacy	Gender, age	Women are more concerns than men about privacy (p < .05), age is positively associated with privacy concern (r = .10, p < .01).
Junglas et al. [2008]	CFIP	Big Five personality traits	Agreeableness (β = -.22, p < .01) is negatively associated with CFIP; conscientiousness (β = .12, p < .05) and openness to experience (β = .11, p < .05) are positively associated with CFIP.
Kim et al. [2008b]	Privacy concerns	Education intervention	The education intervention tested does not have a significant impact on privacy concerns.
Korzaan and Boswell [2008]	CFIP	Big Five personality traits, and Computer anxiety	Agreeableness has a positive impact on CFIP (β = .17, p < .027). The impacts of extraversion, conscientiousness, and computer anxiety on CFIP are not supported.
Laric et al. [2009]	Concerns for healthcare information privacy	Gender, age, race, and health insurance coverage	Overall, women are more concerned about healthcare information privacy than men, and older people are more concerned than younger people. Race also plays some roles in privacy concerns, but insurance coverage has no impact on privacy concern.
Lee and Cranage [in press]	Privacy concerns	The combination of personalization with privacy assurance	Only privacy assurance has a main effect on privacy concerns (F = 16.11, p < .001).
Lwin et al. [2007]	Online privacy concerns	Perceived company privacy policy, perceived online privacy government regulation, and congruency (relevance of data to transaction)	Policy (F = 9.6, p < 0.001), regulation (F = 14.1, p < 0.001) and congruency each have a significant impact on privacy concern.
Milberg et al. [2000]	Internet Users' Information Privacy Concerns (IUIPC)	Culture values	Culture values have a strong impact on CFIP (β = .13, p < .05); specifically, power distance, individualism, and masculinity each have a positive effect on CFIP, whereas uncertainty avoidance has a negative relationship with CFIP.
Nam et al. [2006]	Privacy concerns	Perceived convenience of a website, reputation of a website, and 3rd party certificate in a website	Both perceived convenience (β = -.44, p < .01) and 3rd party certificate (β = -.14, p < .05) have a negative impact on privacy concerns, but reputation has no significant impact.
Okazaki et al. [2009]	Privacy concerns	Prior negative experience	Prior negative experience in personal information disclosure increases mobile users' information privacy concerns (β = .18, p < .001).
Pavlou et al. [2007]	Information privacy concerns	Website informativeness, Trust, and Social presence	Website informativeness has a negative impact of on CFIP (β = -.21, p < .01; β = -.23, p < .01); trust has a negative impact on CFIP (β = -.36, p < .01; β = -.30, p < .01); social presence has a negative impact on CFIP (β = -.14, p < .05;β = -.28, p < .01).
Phelps et al. [2001]	Privacy concerns	Desired information control, and attitude toward direct marketing	Consumers' attitudes toward direct marketing (β = -.106, p < .1) and their desire for control over personal information (β = .425, p < .1) are significantly related to their level of privacy concern.
Rohm and Milne [2004]	Privacy concerns regarding specific types of information	Sources of information, types of information, relationship with the organization	Consumers are more concerned about organizations obtaining their personal information from medical records than from other sources. They are also more concerned if organizations purchased a list with their personal medical history rather than a list with other types of information. The influence of a person's ongoing relationship with a company has a mixed impact on their privacy concerns.

Table B-1: Antecedents of the Privacy Construct - Continued

Sheehan [1999]	Privacy concerns	Gender	In general, women are more concerned about online privacy than men.
Smith et al. [1996]	CFIP	Previous experience with information misuse, Knowledge of media coverage, Cynical distrust, Paranoia, and Social criticism	Previous experience (β = .16, p < .01), knowledge of media coverage (β = .22, p < .01), cynical distrust (r = .30, p < .05), paranoia (r = .37, p < .001) and social criticism (r = .37, p < .001) each have a positive relationship with CFIP.
Stewart and Segars [2002]	CFIP	Computer anxiety	Computer anxiety has a positive impact on CFIP (β = .72).
Tsarenko and Tojib [2009]	Privacy concerns	Trust, concern with privacy statements, government protection of privacy, and willingness to disclose for compensation.	Trust (β = -.478, t = -13.86) and government protection of privacy (β = -.073, t = -2.05) each have a negative impact on privacy concern; concern with privacy statements has a positive impact on privacy concern (β = .181, t = 5.33); willingness to disclose for compensation is, however, positively associated with privacy concern (β = .218, t = 5.15)
Ward et al. [2005]	Privacy concerns	Types of information requested (financial and personally identifiable), provision of benefits (discount and personalized service), degree of Internet use, online purchase experience, and level of materialism	Only request for financial information and materialism have significant impact on privacy concerns.
Wirtz et al. [2007]	Privacy concerns	Perceived responsibility of an organization to protect privacy, and perceived effectiveness of the regulatory framework for protecting privacy	Both organizational policy (β = -0.41, p < 0.01) and regulation (β = -0.42, p < 0.01) are negatively associated with privacy concerns.
Xu [2007]	Privacy concerns	Perceived control	Perceived control has a negative impact on privacy concerns (Split groups: β = -.67 and β = -.75, p < .01).
Xu and Teo [2004]	Privacy concerns	Technology-based control, institution-based self-regulation, and legislation	Technology (β = -0.358, p < .05), self-regulation (β = -0.107, p < .05) and legislation (β = -0.098, p < .05) each have a significant impact on privacy concerns.
Xu et al. [2008]	Privacy concerns	Privacy risk, perception of intrusion, and privacy control	Intrusion and privacy risk have positive impacts on CFIP, and privacy control has a negative impact. Each of the three antecedents are influenced by other factors such as privacy awareness, privacy social norm, privacy policy and industry self-regulation
Yang and Wang [2009]	CFIP	Information sensitivity, and Compensation	Information sensitivity does not have a significant impact on privacy concern. Compensation does not have a significant impact on privacy concern.
Yao et al. [2007]	Concerns about online privacy	Psychological need for privacy, Beliefs in privacy rights, Internet use fluency, Internet use diversity, General self-efficacy, and Gender	Psychological need for privacy has a positive impact on CFIP (β = .19); beliefs in privacy rights has a positive impact (β = .38); general self-efficacy has a negative impact (β = -.07, p = .1). Other antecedents are not found to have a significant impact on CFIP.
Yao and Zhang [2008]	Privacy concerns	Internet use frequency, fluency, diversity, belief in privacy right, and need for privacy	Internet use frequency (β = .11, p < .05), fluency (β = .09, p < .1), diversity (β = -.14, p < .01), and belief in privacy right (β = .46, p < .001) each have a significant impact on privacy concern. The impact of need for privacy on privacy concern is mediated by privacy right.
Youn [2008]	Teens' privacy concerns	Perceived parental mediation (rule-making, co-surfing, and parent-child discussion) of privacy	Co-surfing (β = .119, p = .026) and parent-child discussion (β = .233, p < .001) have positive impacts on privacy concern. Rule-making does not have a significant impact.
Youn [2009]	Privacy concerns	Perceived risks of information disclosure (vulnerability to risks), perceived benefits, privacy self-efficacy, gender, duration of Internet use, persuasion knowledge, and privacy knowledge	Perceived vulnerability to privacy risks was positively related to the level of privacy concerns (β = .366, p < .001). Perceived benefits were negatively related to the level of privacy concern (β = -209, p < .05). Girls show more concerns about privacy than boys (β = .205, p < .05). None of the other antecedents have significant impact on privacy concerns.

Table B-1: Antecedents of the Privacy Construct - Continued

Yousafzai et al. [2009]	Perceived privacy	Perceived trustworthiness of a bank	Perceived trustworthiness has a positive impact on perceived risk (β = .60, t = 11.90)
Zhang et al. [2002]	Privacy concerns	Age, education, income, online shopping experience, gender	U.S. Study: Age, online shopping experience and gender have impacts on certain aspects of privacy concerns; education and income have no significant impact on the concerns. China study: Age has a negative impact on privacy concern, which is in contrast to the results from US study; income has an important impact on privacy concerns.
Zviran [2008]	Privacy concerns	Use of privacy enhancing mechanisms, Previous experience with online privacy invasion, Web usage, Web skills, and Web experiences	CFIP is positively related to use of privacy enhancing mechanisms, previous experience, and Web usage. No significant relationship exists between CFIP and Web skills, or between CFIP and Web experiences.

APPENDIX C: CONSEQUENCES OF CFIP

Table C-1: Consequences of CFIP

Literature	Privacy construct	Consequences	Major findings
Angst and Agarwal [2009]	CFIP	Opt-in intention	CFIP is negatively associated with opt-in intention / likelihood of adoption (β = -.107, p < .05).
Ashley et al. [in press]	Privacy concerns	Customer Relationship Program Receptiveness (RPR)	Privacy concerns have a negative effect on RPR (β = −.11, p < .05).
Awad and Krishnan [2006]	Privacy concerns	Perceived importance of information transparency	CFIP is positively associated with perceived importance of information transparency (β = .03), which in turn interprets the willingness to be profiled for personalized online service and advertising.
Bansal et al. [2010]	Health information privacy concerns	Trust in the health website and intention to disclose health information	Health information privacy concern has a negative impact on intention to disclose health information (β = -.27, p < .001), but the privacy concern has no significant impact on trust.
Casalo et al. [2007]	Perceived website privacy	Trust	Perceived privacy and security has a positive impact on trust in a financial service website (β = .664, p < .01).
Cases et al. [2010]	Perceived privacy concerns	Website trust, intention to return to the company's website, and attitude toward the website	Low perceived privacy concerns (measured as perceived privacy) lead to more trust in the website (β = .23, p < .01) and better attitude toward the website (β = .22, p < .01), but privacy concerns have no significant impact on intention to turn to the site. Trust and attitude, nevertheless, both have a positive impact on intention.
Cazier et al. [2008]	Perceived privacy risk likelihood and perceived privacy risk harm	Intention to use RFID	Both perceived privacy risk likelihood (β = -.46, p < .01) and perceived privacy risk harm (β = -.15, p < .05) have a negative impact on intention to use RFID
Chen and Rea [2004]	Privacy concerns	Use of privacy control techniques (falsification, passive reaction, and identity modification)	Neither types of privacy concerns (i.e., unauthorized use and giving out information) are strongly associated with falsification; concerns about unauthorized use is positively associated with passive reaction (β = .43, t = 3.40); concern about giving out information is, however, negatively associated with identity modification (β = -.40, t = -.2.28).
Cheung and Liao [2003]	Privacy concerns	Unwillingness to e-shop on the Internet	A positive impact of privacy concerns on the unwillingness to shop on the Internet (β = .189, p < .01) was observed.
Chiu et al. [2009]	Privacy	Trust in the online vendor	Privacy has a positive impact on trust (β = .19, p < .01)
Cocosila et al. [2009]	Perceived privacy risks	perceived psychological risk	Perceived privacy risk has a positive impact on perceived psychological risk (β = .444, p < .001)
Dai and Palvia [2009]	Privacy perception	Intention to adopt mobile commerce	Privacy perception has a positive impact on the intention to use in the US sample (β = -.164, p < .01), but not in the China sample (β = .056, n.s.).

Table C-1: Consequences of CFIP - Continued

Dinev et al. [2006]	Privacy concerns	E-commerce use	Privacy concern is negatively associated with e-commerce use (Italy—$\beta = -.14$, $p < .01$; U.S.—$\beta = -.38$, $p < .01$)
Dinev and Hart [2005]	Internet privacy concerns	Intention to transact	Privacy concern is negatively associated with intention to transact ($\beta = -.39$, $p < .01$)
Dinev and Hart [2006]	Internet privacy concerns	Willingness to provide information to transact	Privacy concern is negatively associated with the willingness to provide information to transact ($\beta = -.38$, $p < .01$)
Dinev et al. [2008]	Internet privacy concerns	Willingness to provide personal information to transact	Both dimensions of CFIP, finding and abuse, are negatively related to willingness to transact ($\beta = -.24$, $p < .01$; $\beta = -.22$, $p < .01$).
Eastlick et al. [2006]	Privacy concerns	Trust on an e-commerce website, Intention to purchase from the website	Privacy concerns has a negative impact on trust ($\beta = -.50$, $p < .001$), and has a negative impact on the intention to purchase ($\beta = -.23$, $p < .001$)
Faja and Trimi [2006]	General CFIP and perceived information privacy	Willingness to disclose personal information, and Willingness to buy	General CFIP has negative impacts on the willingness to disclose information and the willingness to buy. Site-specific privacy perception has positive impacts on the willingness to disclose information and willingness to buy.
Frye and Dornisch [2010]	Perceived privacy of a medium	Comfort of disclosing information via instant messaging	Privacy of medium has a positive impact on comfort of disclosing information ($\beta = .31$, $t = 14.24$)
Hui et al. [2007]	Privacy concerns	Information disclosure	Controlling other variables, privacy concerns are not significantly associated with disclosure.
Janda [2008]	Privacy concerns	Likelihood of making online purchases	Privacy concerns have a significant impact on women's likelihood to purchase ($\beta = 0.63$, $p < .01$), but not for men.
Joinson et al. [2010]	Privacy dispositions and perceived privacy	Nondisclosure behavior	Privacy concern has a positive impact on nondisclosure ($\beta = .03$, $t = 2.20$), but the impact of perceived privacy on nondisclosure is mediated by trust. In addition, privacy concern did not predict perceived privacy.
Kim [2008]	Privacy concerns	Trust in e-vendor	Privacy concern has a negative impact on trust in e-vendor, but only in the U.S. sample ($\beta = -.12$, $p < .05$). The relationship is not significant in the South Korea sample.
Kim et al. [2008a]	Perceived privacy protections	Perceived trust and perceived risk	Perceived privacy protection has positive impacts on perceived trust ($\beta = .494$, $p < .001$) and perceived risk ($\beta = -.216$, $p < .01$)
Kim et al. [2008b]	Privacy concerns	Awareness of Web Assurance Seal Services (WASS)	CFIP does not have a significant impact on the awareness of WASS. The other antecedent, security concern, does.
Korzaan and Boswell [2008]	CFIP	Behavioral intention to protect personal information	CFIP has a positive impact on behavioral intention to protect personal information ($\beta = .34$, $p < .001$)
Krohn et al. [2002]	Privacy concerns	Attitude to the Web, Web purchase, we use, and satisfaction	Privacy concern is negatively associated with Web purchase ($\beta = 2.02$, $p < .01$), but not with other dependent variables.
Kumar et al. [2008]	CFIP	Perceived usefulness of firewalls, Attitude toward using firewalls	CFIP has a positive impact on perceived usefulness of firewalls ($\beta = .22$, $p < .05$). No significant relationship is observed between CFIP and attitudes.
Lee and Cranage [in press]	Privacy concerns	Willingness to share personal information and intention to adopt service	Privacy concern has a negative impact on willingness to share identifiable and unidentifiable information ($\beta = -.41$, $p < .001$; $\beta = -.44$, $p < .001$), and also has a negative impact on the intention to adopt service ($\beta = -.37$, $p < .001$).
Li et al. [2009]	Perceived privacy	Swift trust	Perceived privacy has no significant impact on swift trust, but perceived security does.
Lian and Lin [2008]	Privacy concerns	Attitudes toward online shopping	Privacy concerns have a negative impact on the attitude toward purchasing books ($\beta = -.24$, $p = .04$) and TV games ($\beta = -.26$, $p = .02$) online, but not for the purchase of magazines or computer games online.
Liu et al. [2004]	Perceived privacy	Trust on a website	Perceived privacy is positively associated with trust on a website ($r = .75$, $p < .001$)
Liu et al. [2005]	Perceived privacy	Trust	Privacy concern has a strong impact on the trust of an online business ($\beta = .86$)

Table C-1: Consequences of CFIP - Continued

Lwin et al. [2007]	Online privacy concerns	Protective responses of users: fabricating, protecting with technology, and withholding	Privacy concern has a significant impact on each of the protective responses (F = 80.1, 94.5, and 63.2, respectively; $p < .001$).
Malhotra et al. [2004]	Internet Users' Information Privacy Concerns (IUIPC)	Trusting belief an Risk belief	IUIPC negatively influences trusting belief of a firm to protect personal information ($\beta = -.34$, $p < .001$) and positively influences risk beliefs of a high potential for loss of personal information ($\beta = .26$, $p < .001$)
Nam et al. [2006]	Privacy concerns	Willingness to disclose personal information	Privacy concern has a negative impact on the willingness to provide personal information ($\beta = -.15$, $p < .01$).
Okazaki et al. [2009]	Privacy concerns	Trust and perceived risk in mobile advertising	Information privacy concerns decrease mobile users' trust in mobile advertising ($\beta = -.34$, $p < .001$) and increase their perceived risk ($\beta = .74$, $p < .001$).
Pavlou et al. [2007]	Information privacy concerns	Perceived uncertainty	CFIP positively influence perceived uncertainty in online transaction ($\beta = .19$, $p < .01$; $\beta = .15$, $p < .05$)
Phelps et al. [2001]	Privacy concerns	Intensity of catalog purchase behavior	Increasing levels of concern for privacy diminishes the intensity of catalog purchase behavior ($\beta = -1.073$, $p < .1$).
Premazzi et al. [2010]	Privacy concerns	Willingness to provide information and actual behavior of information disclosure	Privacy concern has a negative impact on willing to provide information ($\beta = –0.245$) but does not have a significant impact on the actual behavior.
Roca et al. [2009]	Perceived privacy	Perceived trust	Perceived privacy does not have a significant impact on perceived trust; the other antecedent, perceived security, does.
Sheehan and Hoy [1999]	Privacy concerns	Online behaviors: e.g., registering, providing inaccurate and incomplete information, and read unsolicited e-mail, etc.	Privacy concern has a significant impact on each of the protective behaviors.
Sheng et al. [2008]	Privacy concerns	Intention to adopt personalized service	Privacy concern has a negative impact on intention to adopt personalized services ($\beta = -.475$, $p < .001$; $\beta = -.38$, $p < .001$); however, there is no significant relationship between privacy concerns and intention to adopt non-personalized services
Shin [2010]	Perceived privacy	Perceived security and trust in social networking site, and attitude toward social networking site	Perceived privacy is positively associated with perceived security ($\beta = .50$, $p < .001$), trust ($\beta = .26$, $p < .05$), and attitude ($\beta = .47$, $p < .05$).
Smith et al. [1996]	CFIP	Behavioral intention	CFIP has a positive relationship with the intentions to take privacy-related actions (such as refusal to give information, removal of personal information, and complaining of misconduct, etc.)
Son and Kim [2008]	Information privacy concerns	Information provision, private action, and public action	CFIP has a positive impact on refusal to provide information ($\beta = .33$), removal of personal information ($\beta = .28$), negative word of mouth ($\beta = .27$), complaining to the company ($\beta = .26$), and complaining to third parties ($\beta = .25$), but not on misrepresentation.
Stewart and Segars [2002]	CFIP	Behavioral intention to take privacy-related actions	CFIP has a positive impact on behavioral intentions ($\beta = .71$)
Stutzman et al. [2011]	Privacy attitude	Privacy protective behavior, privacy policy reading, and information disclosure. Gender is used as a control variable.	Privacy concern has no significant impact on protective behavior on Facebook.com, but has a positive impact on privacy policy reading ($p = .02$). Privacy concern is also negatively associated with information disclosures ($p = 0.004$). Gender has no significant impact on disclosure.

Table C-1: Consequences of CFIP - Continued

Van Slyke et al. [2006]	CFIP	Trust, Risk perception, and Willingness to transact	To the contrary, CFIP is positively associated with trust (β = .208, p < .01) in Sample 1; the relationship is not significant in Sample 2. CFIP is positively associated with risk perception in Sample 1 (β = .121, p < .05) and non-significant in Sample 2. None of the samples support the impact of CFIP on the willingness to transact.
Wei et al. [2010]	Privacy concerns	User tolerance of SMS ads, likelihood of passing along received SMS ads, and user acceptance of location-based SMS ads	Privacy concern is negative associated with likelihood of passing along received SMS ads (β = -.16, p < .01), but not significantly associated with the other two responses.
Wirtz et al. [2007]	Privacy concerns	Likelihood of the consumer to misrepresent and fabricate personal information, to adopt privacy protection technologies, and to refuse to register or purchase from a website	Privacy concern has a positive impact on fabricating information (β = .45, p < .01), adopting protective technologies (β = .49, p < .01), and withholding purchase (β = .67, p < .01).
Xu and Teo [2004]	Privacy concerns	Intention to use location-based mobile service	Privacy concerns have a negative impact (β = -0.349, p < .05) on the intentions to use location-based mobile service.
Yang and Wang [2009]	CFIP	Information disclosure intention, protection intention, and transaction intention	Privacy concern has a negative impact on intention to disclose information and a positive impact on protection intention, but it does not have significant impact on intention to transact.
Yao and Murphy [2007]	Privacy	Remote electronic voting systems participation intention	Privacy has a positive impact on intention to use remote electronic voting systems, but only for men (β = .36, p < .01).
Youn [2009]	Privacy concerns	Privacy protection behaviors such as fabricating information, seeking for advice, and refraining from Web use	Privacy concerns have a significant impact on privacy-coping behaviors: seeking (β = .353, p < .001), refusing (β = .237, p < .05), and fabricating (β = .189, p < .10).
Yousafzai et al. [2009]	Perceived privacy	Trust	Perceived privacy has a positive impact on trust (β = .27, t = 5.36).
Zimmer et al. [2010]	Information privacy concerns	Intention to disclose personal information	CFIP has a negative impact on intention (β = -.21, p < .01)
Zviran [2008]	Privacy concerns	Canceling online spending, Refraining from surfing, and Volume of online spending	CFIP has a significant impact on refraining of surfing. However, relationships between CFIP and canceling online spending and the volume are not significant.

APPENDIX D: MODERATING EFFECTS INVOLVING CFIP

Table D-1: Moderating Effects Involving CFIP

Literature	Privacy construct	Other constructs	Major findings
Angst and Agarwal [2009]	CFIP	Argument frame, issue involvement, and the interaction between argument frame and issue involvement	CFIP moderates (1) the relationship between argument frame and post-attitude (β = –.530, p < .001), (2) the relationship between issue involvement and post-attitude (β = –.122, P < .01), and (3) the impact of the interaction between argument frame and issue involvement on post-attitude (β = .628, p < .001).
Bansal et al. [2008]	Privacy concerns	Website design quality, privacy policy understandability, adequacy of privacy policy, website information quality, third party endorsements, and company information	CFIP moderates the impact of website design quality on the trust of a website. The moderating effects of CFIP on other variables, including privacy policy understandability, perceived adequacy of privacy policy, perceived website information quality, presence of third-party endorsements and perceived presence of company information, were rejected or mixed.
Culnan and Armstrong [1999]	Privacy concerns	Awareness of procedural fairness of a company	Awareness of procedural fairness moderates the impact of privacy concerns on the willingness to be profiled: for individuals not aware of procedural fairness, privacy concern is a discriminator of the willingness to be profiled; for individuals aware of procedural fairness, privacy concern is not a discriminator.
Faja and Trimi [2006]	General CFIP: and perceived information privacy	Identifiable and non-identifiable information, General CFIP	(1) Identifiable information moderates the impact of site-specific CFIP on the willingness to disclose personal information; non-identifiable information has a moderating effect contrary to the prediction. (2) The moderating effect of General CFIP on the relationship between vendor intervention and site-specific CFIP is non-significant.
Frye and Dornisch [2010]	Perceived privacy of a medium	Topic intimacy, and frequency of use of communication medium	Topic intimacy moderates the impact of perceived privacy on comfort of disclosure (β = .01, t = 3.42). In contrast to expectations, frequency of use weakens the association between privacy and disclosure comfort.
Janda [2008]	Privacy concerns	Gender	For women, privacy concerns have a significant impact on likelihood of purchase (β = -.63, p < .01); for men, the relationship is non-significant.
Lai and Hui [2004]	Privacy concerns	Opt-in and opt-out behavior	Consumers' privacy concerns moderate/reduce the difference between opt-in and opt-out behavior in inducing online activities.
Luo and Seyedian [2003]	Privacy concerns	Perceived importance of contextual marketing and perceived importance of customer orientation	CFIP was not found to moderate the relationship between the perceived importance of contextual marketing and satisfaction with Internet storefronts, or the relationship between the perceived importance of customer orientation and satisfaction.
Lwin et al. [2007]	Online privacy concerns	Information sensitivity	Information sensitivity moderates the impact of privacy policy on privacy concern.
McCole et al. [2010]	Privacy and security concerns	Trust in vendor, trust in the Internet, and trust in third parties	Perceived privacy and security concerns moderates the relationship between (a) trust in a vendor and attitude toward online purchasing (β = .08, t = 1.84); (b) trust in the Internet and attitude toward online purchasing (β = -.11, t = -2.29); and (c) trust in third parties and attitude toward online purchasing (F = 76.2, p < .001). In addition, privacy and security concerns do not have a significant impact on attitude.
Okazaki et al. [2009]	Privacy concerns	Sensitivity of the information request, and perceived ubiquity	The greater the sensitivity of the information request, the stronger the effect of information privacy concerns on trust (t = 4.45, p < .001); the greater the perceived ubiquity, the stronger the effect of information privacy concerns on trust (β = -.13, p < .001). Neither information sensitivity nor perceived ubiquity moderates the association between privacy concerns and perceived risk.

Table D-1: Moderating Effects Involving CFIP - Continued

Rensel et al. [2006]	Task privacy	Individual need for privacy	Individual need for privacy moderates the impact of task privacy, available assistance, and perceived tracking on transactional website use; the moderating effect of individual need for privacy on anonymity was not supported.
Rifon et al. [2005]	Privacy concerns	Privacy seal presence	No significant interactions between seal presence and privacy concern were found for any of the dependent measures: belief in seal assurances, trust, and information disclosures. Nevertheless, privacy concern was found to have significant effects on disclosures of home address and salary information.
Sheng et al. [2008]	Privacy concerns	Context (emergency versus non-emergency)	Context moderates the relationship between personalization and privacy concerns. For non-personalized services, there is no significant difference in privacy concerns between emergency and non-emergency contexts (t = -1.94, p > 0.05); for personalized services, customers' privacy concerns are significantly higher in the non-emergency context than in the emergency context (t = -3.74, p < 0.05).
Van Slyke et al. [2006]	CFIP	Familiarity	The moderating effects of familiarity on the relationship between CFIP and trust, and between CFIP and risk perception, are unsupported.

ABOUT THE AUTHOR

Yuan Li is an assistant professor in the Division of Business, Mathematics and Sciences at Columbia College in Columbia, South Carolina. He received his Ph.D. in Management Information Systems from the University of South Carolina. His current research focuses on knowledge management at the organizational and individual levels, knowledge and skills transfer in end user computing, and online information privacy. His research appeared or is forthcoming in the *Journal of the Association for Information Systems*, *European Journal of Information Systems*, and the *Journal of Organizational and End User Computing*.

Communications of the Association for Information Systems

ISSN: 1529-3181