Measuring Online Consumer Perceptions of Fair Information Practices

By

Jiawei Liao

Bachelor of Economics, University of International Business and Economics, 1996

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

In

THE FACULTY OF GRADUATE STUDIES

Sauder School of Business

We accept this thesis as conforming to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

December 2003

Library Authorization

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

JIAWEI LIAO — Name of Author *(please print)*

4/01/2004 — Date (dd/mm/yyyy)

Title of Thesis: Measuring Online Consumer Perceptions of Fair Information Practices

Degree: Master of Science Year: 2004

Department of Commerce
The University of British Columbia
Vancouver, BC Canada

ABSTRACT:

The expansion of e-commerce has made consumer privacy issues more salient and pressing. Previous studies of online commerce have indicated that limited confidence in privacy protection has been a major problem impeding the growth of e-commerce. The United States Federal Trade Commission developed the Fair Information Practice Principles in its 1998 report to congress to ensure that the collection and use of personal information is conducted fairly, and to provide sufficient privacy protection for consumers. The Federal Trade Commission's core principles are notice, choice, access, and security.

The purpose of this study is to develop an instrument to measure the degree to which online entities adhere to fair information practice principles, from the perspective of consumers. The instrument development process included three stages: item creation, card sorting, and instrument testing. First, we generated 25 items based on the definitions of the four fair information principles. Then, we asked eight judges to sort the items into various categories, and according to the card sorting results, we deleted some poor items from the scales. Finally, we conducted an online survey to test the instrument. We applied factor analysis and other validity and reliability analyses to the survey data, resulting a validated 23-item, five-scale instrument. This instrument can be used to evaluate the privacy protection practices of online entities, and to judge from the consumers' perspective if these practices are fair and provide sufficient protection.

Table of Contents

List of Tables

List of Figures

Acknowledgement

The author wishes to express her gratitude to Professor Jai Yeol Son and Izak Benbasat for their guidance and supervision of this thesis, and Professor Paul Chwelos for his role as an external examiner. In addition, the author would like to thank Dave Hood for his input in the item creation process, and Yali Zhang, Lingling Tu, Irene Pan, Weida Wang, Lingyun Qiu, Jack Jiang, Weiquan Wang and Lei Zhu for their input in the card-sorting process as judges.

1.0 Introduction

Over the past decade the expansion of e-commerce has changed the processes and uses of consumer data collection, making the consumer privacy issues more salient and pressing. According to a recent edition of *E-Stats* (U.S. Department of Commerce, 2001), online retail sales in 2001 accounted for 1.1 percent ($34 billion) of total retail sales in the United States, an increase of 22 percent over the $28 billion of online sales in 2000 (0.9 percent of total retail sales). The relatively small share of e-commerce indicates that it continues to have enormous potential to grow; however, previous studies of online commerce have indicated that limited confidence in privacy protection has been a major problem impeding its growth. According to the Federal Trade Commission (2000), many consumers never shop online, because they are concerned about their privacy. Furthermore, this report indicated that one study[1] estimated that privacy concerns may have caused a $2.8 billion loss in online retail sales in 1999. The same report cited results from a study conducted by Jupiter Communications[2], which suggested that privacy concerns could cause losses of up to $18 billion by 2002, from a projection of $40 billion in potential total online sales, if no systematic actions were taken to relieve consumer privacy concerns. A recent survey stated that,

> "Overall, 88.8 percent of all respondents age 16 or over in 2002 expressed some concern about the privacy of their personal information when or if they buy on the Internet... More specifically, 54.3 percent said they are very concerned or

[1] Forrester Privacy Best Practice Report (cited in Microsoft Advertisement, N.Y. Times, Mar. 23, 2000, A12)
[2] Overview: Proactive Online Privacy: Scripting an Informed Dialogue to Allay Consumers' Fears, available at <http://www.jup.com>.

extremely concerned about the privacy of their personal information when buying online" (UCLA Center for Communication Policy, 2003, p 49).

Thus, if online sales are to be maximized, online consumers must be assured that their privacy is properly protected.

Since the time of direct mail, many studies have addressed privacy issues. Some have focused on factors underlying consumer privacy concerns, while others have placed more emphasis on marketing practices. Culnan and Armstrong (1999) have indicated that organizations can address privacy concerns and retain customers by observing "procedural fairness", which refers to the perception by the participant that a particular activity is conducted fairly.

The United States Federal Trade Commission (FTC) has studied online privacy issues since 1995. Fair information practice principles, as described in a 1998 FTC report, were developed to ensure that practices related to the collection and use of personal information remain fair, and to provide sufficient privacy protection for consumers. The FTC relies on these principles to guide industry self-regulation for privacy protection. The FTC's fair information practice principles are divided into four categories: notice, choice, access, and security. These principles will be described in the next section of this paper.

The FTC's principles for fair information practices have been widely accepted in public policy, and have been used to evaluate industry efforts in privacy practices from the

marketers' perspective. However, beyond the guidelines addressed by the FTC principles, some individual consumers want opportunities to assess online privacy protection efforts, and some online marketers want to know if consumers will have enough confidence in their privacy policies when they implement the FTC core principles. To answer these questions, this study will develop an instrument to measure the degree to which an online entity adheres to fair information practice principles, from the perspective of consumers. The instrument will identify concerns about online privacy, and it could be used in the following circumstances:

(1) Online consumers can use the instrument to evaluate web sites and to judge if practices and systems that protect privacy are fair and adequate.
(2) Online marketers can use the instrument to evaluate their own consumer privacy protection practices, and to judge if these practices are fair and provide sufficient protection to consumers.

"Information privacy" refers to individuals' rights to exclusively control the information about them. It can be applied when other organizations or people attempt to collect, use and distribute personal information (Malhotra *et al*, 2003). Concern for Information Privacy (CFIP) instrument, constructed by Smith *et al.* (1996), is an existing measurement for information privacy concerns. The CFIP instrument consists of four constructs and fifteen items. It was developed to capture individual's concerns towards organizational information privacy practices. Though both the CFIP instrument and our instrument under development can be used to measure the individuals' perception of

organizations' information privacy practices, CFIP might not be suitable to measure the information privacy concerns of Internet users since CFIP instrument was developed in a conventional (offline) context. Compared to the traditional media, the Internet makes it much easier to perform two way communications between consumers and organizations (Hoffman and Novak 1996), which means that the Internet provides a more convenient way for the consumers to manage personal information. Accordingly, we develop the FTC instrument in an online environment and take more consideration of the interfaces between consumers and online companies.

This paper reports the process and results of the development of an instrument to measure online consumers' perceptions of the online entities implementing FTC's fair information practice principles. The next section includes a detailed description of fair information practice principles, a review of Concern for Information Privacy (CFIP) instrument, and a selection of studies related to online privacy concerns. Chapter 3 describes the methodology, process and results of the instrument development process, followed in Chapter 4 by a discussion of the results, limitations of the study, and suggestions for future research.

2.0 Literature Review

2.1 FTC Fair Information Practice Principles

Fair information practices have been defined in Culnan and Armstrong (1999) as the procedures that provide individuals control over the disclosure and secondary uses of their own personal information, and the authors have identified the core of fair information practices as (1) notice, and (2) consent. The results of this study indicate that when consumers are explicitly informed regarding the fair information practices being implemented, privacy concerns do not affect their willingness to give out personal information.

The Federal Trade Commission has studied online privacy issues since 1995. In "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress" (2000), the FTC has identified four widely accepted categories of fair information practice principles related to the collection, use and dissemination of personal information: notice, choice, access, and security. In FTC documents, "personal information" was defined to include any identifying information, demographic information or preference information. The FTC has defined the categories in the following terms:

(1) *Notice*. Organizations operating online should inform consumers about their information practices before collecting any personal information. A notice should clearly identify some or all of the following: who is collecting the information, the

intended uses for the information, any and all potential recipients of the information, any concealed or secondary means of collection, and whether the personal information is voluntary or required. It should also clearly state the processes involved to ensure the confidentiality, integrity and quality of the data.

(2) *Choice*. Consumers should be provided with simple, accessible and affordable mechanisms enabling them to determine how their personal information will be used and disseminated. Such choices may include dissemination to internal secondary uses (e.g. marketing to current consumers) or external secondary uses (e.g. sharing data with third parties).

(3) *Access*. Consumers should be able to access their own information and to correct inaccuracies or delete information.

(4) *Security*. The online organizations should assure the accuracy, completeness, and consistency of data; and they should protect the data from loss, misuse and destruction.

As indicated in 2000 FTC report, consumer-oriented commercial web sites that collect personal identification information online would be required to comply with these four fair information practice principles.

To examine the status of online privacy and the effectiveness of industry self-regulation, the FTC conducted online privacy surveys in 1998 and 2000. In the 1998 online privacy survey of commercial web sites, only a few (14 percent of the comprehensive random sample) disclosed any of their information practices, while most (92 percent) collected

personal information from consumers. In addition to counting disclosures, the FTC's 2000 survey also analyzed the nature and substance of the privacy disclosures according to the fair information practice principles of notice, choice, access and security. It found that only 20 percent of the random web site sample implemented at least part of all four principles, and only 41 percent met the basic notice and choice standards. The survey results demonstrated that industry efforts alone were not sufficient, and legislation was necessary to ensure the further implementation of fair information practices online. The FTC 2000 report also indicated that, "the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations."

2.2 Existing Measurement Instruments for Privacy Concerns– Concern for Information Privacy Instrument

The Concern for Information Privacy (CFIP) instrument (see Appendix 1), as constructed by Smith *et al.* (1996), is a fifteen-item instrument that reflects four dimensions of information privacy concern: collection, error, secondary use, and unauthorized access. "Collection" refers to the consumer perception that too much personal information is collected (the FTC has not identified a related principle). "Error" refers to concerns that companies should have proper procedures to minimize errors in personal data; this is relevant to the FTC's core principle of security. "Secondary use" refers to concerns about information being used for purposes other than the initial reasons it is collected; this is relevant to the FTC's core principle of choice. "Unauthorized access" refers to concerns

that people without authorization might have access to personal information; this is relevant to the FTC's principle of security. The CFIP instrument was first developed by Smith *et al.* (1996) to measure the primary dimensions of individuals' concerns about organizational information privacy practices. Stewart and Segars (2002) have further developed the CFIP instrument by testing it in a theoretical framework, and by examining its dimensionality, reliability, and validity.

The CFIP instrument was developed in the context of conventional (i.e. not online) commerce. Stewart and Segars (2002) adapted it to online contexts. They identified CFIP as a consequence of "computer anxiety" and a predictor of "behavioural intention". Their results have revealed that consumers are concerned about all dimensions of corporate information practices, rather than any particular one, and therefore the interrelationship among the four factors considered by CFIP is an important component of the instrument. These conclusions indicate that CFIP might be better represented in a higher order factor structure. The findings also suggested that the central concern underlying consumer attitudes about information privacy is the issue of control.

2.3 Applicability of Research into Conventional Privacy Issues to E-commerce Environments

2.3.1 Dimensions of Online Privacy Concerns

Privacy research has expanded since the early 1990s, particularly in the context of direct marketing. Many of the findings related to concerns about privacy in previous studies

conducted in the context of traditional direct marketing can be applied to online environments. Notably, Sheehan and Hoy (2000) examined the extent to which existing knowledge about privacy in traditional direct marketing can be applied to the online context, and they have assessed the current FTC privacy policies in this light. Previous marketing studies have indicated that two dimensions of control, "awareness of information collection" and "usage beyond original transaction", are the most prevalent influences on consumer concerns about privacy, and they are the foundation for the FTC's core principles of online information collection. However, the contextual nature of privacy is more complex. Three other dimensions that may influence privacy concerns have also been identified: "how sensitive the person considers the information, how familiar the person is with the entity collecting the information and what compensation is being offered to the person in exchange for the information" (Sheehan and Hoy, 2000, p. 66). Based on an extensive literature review, Sheehan and Hoy have proposed five dimensions for consumer concerns about privacy:

(1) *Awareness of information collection.* This is related to the FTC's principle of notice.

(2) *Information usage*. This refers to the purposes for which marketers use consumer information and how they use the information. It is related to the FTC's principle of choice.

(3) *Information sensitivity*. This is contextual. Consumers may show contrasting levels of sensitivity among different type of information.

(4) *Familiarity with entity*. This refers to consumer knowledge of, and familiarity with, the organizations requesting their personal information.

(5) *Compensation.* This refers to consumer expectations regarding what they will gain through their interactions with the organization requesting their information.

An e-mail survey has been conducted with a national probability sample of 889 online users to test if these five influences reflect the underlying dimensions of consumer privacy. The results of factor analysis have indicated that there are three factors influencing consumer privacy online:

(1) *Control over collection and usage of information.* This factor provides the strongest explanation for concerns about privacy, and therefore is at the heart of the current FTC guidelines. It is directly relevant to the FTC's core principles of notice and choice.

(2) *Short-term, transactional relationship (issue of exchange).* This factor indicates the contextual nature of concerns about online privacy. Online users may balance the information they give out with what they may receive in exchange. This study suggests that the "issue of exchange" can be added to the FTC's core principles.

(3) *Established, long-term relationship.* This factor suggests that mutually beneficial relationships between consumers and online entities influence concerns about privacy.

2.3.2 Internet Users' Information Privacy Concerns (IUIPC)

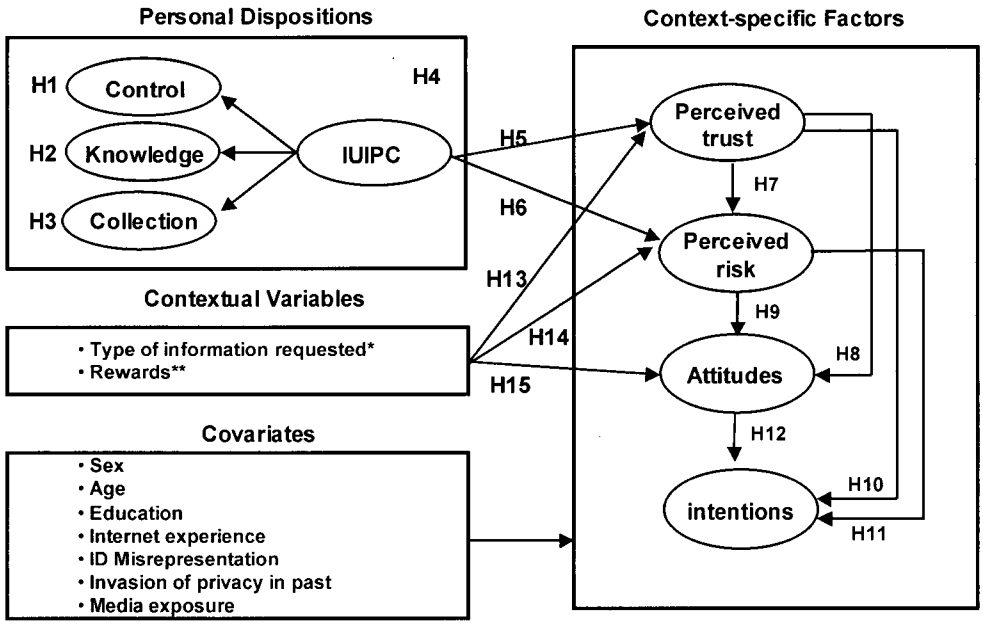
Malhotra, Kim and Agarwal (2003) have also attempted to extend the previous findings regarding consumer privacy concerns to the Internet environment. In particular, they have

attempted (1) to conceptualize Internet users' concerns about information privacy and to propose a theoretical framework for understanding these concerns; (2) to develop a scale for measuring Internet users' information privacy concerns; and (3) to test a nomological framework for consumer attitudes and reactions to online information privacy-related issues.

Malhotra *et al.*'s (2003) study defined the construct of Internet Users' Information Privacy Concerns (IUIPC), and it developed a scale based on exchange theory, social contract theory and the concern for information privacy (CFIP). The study used a social contract theoretical framework (Milne and Gordon, 1993) to explain the three underlying dimensions of online privacy concern: control, knowledge, and collection. The issue of control refers to consumers' perceptions of the importance of controlling their own personal information. Control is often exercised through approval, modification, or opt-in and opt-out options, and therefore it is relevant to the FTC's core principle of choice. The issue of knowledge, on the other hand, relates to consumers' perceptions of how important it is to them to be notified of the methods used for the collection, processing and application of information, and it is relevant to the FTC's core principle of notice. The issue of collection refers to concerns about other parties that might gain possession of personal data, which is relevant to the FTC's core principle of security. The IUIPC construct can be conceptualized as a second-order factor that governs the correlations among control, knowledge and collection.

Malhotra *et al.*'s developed measures for two dimensions of privacy concerns: knowledge and control. The scale for the collection construct was adapted from CFIP instrument (Smith *et al.* 1996) and excluded from their pilot study. A pool of items was created following guidelines introduced by Chin, Gopal, and Salisbury (1997), who developed a scale to measure the faithfulness of appropriation of advanced information technologies, through a process consisting of initial item development, instrument testing and refinement, and confirmatory analysis. After a structured questionnaire was administered in personal, face-to-face interviews and confirmatory factor analysis was performed, six items were left along with the existing four-item collection scale, to formulate the IUIPC construct.

Figure 1. Conceptual Framework on Consumers' Reactions to Online Privacy Threats



Note: This figure is intended to represent a conceptual model, but not a structural equation model.
* insensitive information (0), sensitive information (1)
** Excluded in the empirical test (Set to constant)

(Source: Malhotra *et al.* 2003, p. 14)

Previous studies demonstrated that privacy-related behaviour varies in different contexts. For this reason, Malhotra *et al.* proposed a conceptual model of the relationships among IUIPC, particular contexts and context-specific psychological factors (see Figure 1). Two types of scenarios were used to test the nomological framework, one that involves a request for sensitive personal information (financial information), and another that solicits non-sensitive information (personal shopping preferences). The results of their study indicate no significant direct influence of IUIPC on a consumer's intention to give out information, and no direct relationship between IUIPC and consumer attitudes. These findings suggest that privacy-related behavior depends highly on context, such as the type of information collected.

2.4 Communicating Information Practices with Consumers - Online Retailer Disclosures

One feasible and important way to get impression of how well the web retailers do on privacy protection is to examine their disclosures on the web sties. In fact, disclosure of online privacy practices were the subjects of several online privacy related studies, including the FTC 1998 and 2000 surveys and Georgetown Internet Privacy Policy Study (Culnan, 1999a). Miyazaki and Fernandez (2000) examined online retailer privacy and security disclosures for seventeen product categories, and evaluated potential relationships between these practices and consumer perceptions of risk and purchase intentions across product categories. Their study outlined three key privacy concerns and three security concerns.

Privacy concerns:

(1) *Online customer identification.* Online retailers should disclose their use of cookies and other automatic identification technologies. This related to the FTC fair information practice principle of notice.

(2) *Unsolicited customer contacts.* Retailers should identify their policies regarding the use of information to make unsolicited contacts, beyond the explicit purposes for which the data is initially collected. This concern is covered by the FTC fair information practice principle of choice.

(3) *Customer information distribution.* Retailers should disclose whether they share any information with third parties. This concern is also covered by the FTC fair information practice principle of choice.

Security concerns:

(1) *Security transactions.* As covered by the principle of security.

(2) *Online credit card security guarantees.* This is also covered by the principle of security.

(3) *Alternative payment options.*

Miyazaki and Fernandez examined 381 commercial web sites, and collected descriptive data concerning both the presence of measures for protecting information privacy and the presence of security disclosures. They identified the types and levels of disclosures on the various web sites. To apply their findings, they compared the prevalence of disclosures to a subset of data from a March 1999 consumer survey, a pencil-and-paper questionnaire completed by 160 Internet users. The purpose of this survey is to explore online

consumers' activities and perceptions. In the 1999 survey, they measured purchase likelihood and risk perception for 17 categories of goods sold online and those categories were also used in the web site examination process. The results indicate that there is no relationship connecting consumer perceptions of risk either to privacy or to security. However, they observed that within particular categories, both privacy statements and security statements are positively related to the likelihood that purchases will be completed on particular web sites.

2.5 Previous surveys based on FTC Fair Information Practice Principles

Based on the Federal Trade Commission core principles of fair information practices, the FTC and Georgetown University examined commercial web sites in 2000 and 1999, respectively, to assess industry practices related to privacy protection. They sought to determine whether consumer privacy online can be protected through self-regulation, or whether government intervention is needed. These studies have used content analysis to assess the efforts made by online entities, from the perspective of the businesses operating web sites.

The Georgetown Internet Privacy Policy Study (Culnan, 1999a) surveyed a random sample of 361 commercial U.S. web sites, assessing the extent to which consumer-oriented commercial web sites post privacy policies, and whether these policies reflect fair information practices. The questionnaire used in the study included a section about the content of disclosures, designed to measure the extent to which the privacy

disclosures posted by web sites are based on fair information practices. The questionnaire translated the FTC core principle requirements into a coding scheme. For example, there is a requirement of the principle of notice: "identification of the uses to which the data will be put." (FTC 1998 report, p.7) In the coding scheme it is represented in question 25 of Part V: "Does the site say how the information it collects from consumers will be used?" (Culnan 1999a, p. 50) Though the goal and perspective of Georgetown survey were different from the study described in this paper, the questionnaire was a useful reference during the development of our instrument. Culnan (1998) outlined a methodology for assessing the implementation of self-regulation, defined by the "Elements of Effective Self-Regulation for Protection of Privacy" (US Department of Commerce, 1998), which are almost identical to the FTC's core principles of fair information practice. She used content analysis to audit the content of disclosures on web sites against the requirements of the Elements paper, and collecting data through the analysis of web site content. To assess the implementation of privacy protection on fair information practices and enforcement, she developed a checklist by translating the detailed requirements of fair information practices contained in the Element paper into checklist items. The items in the self-regulation checklist were referred to in the generation of the items for the FTC instrument under development.

Table 1 summarizes the purposes, methodologies and key findings of previous studies related to online information privacy concerns, as described in the above section.

Table 1: Summary of Previous Studies about Online Information Privacy Concerns

Study	Purpose	Focus	Methodology	Key Findings
Culnan & Armstrong, 1999	To investigate relationships between procedural fairness and consumer privacy concerns	Test hypothesis: Consumers will be willing to disclose personal information when their concerns about privacy are relieved by their impressions of procedural fairness	Based on a new analysis data from the 1994 Harris Survey on Interactive Service, Consumers and Privacy	When consumers are explicitly notified of the implementation of fair information practices, concerns about privacy do not affect their willingness to submit personal information
FTC Report to congress, 1998 and 2000	To define privacy rules for a self-regulatory regime	Business practices in collecting and using personal information	Content analysis	Four fair information practice principles are summarized: • Notice • Choice • Access • Security
Culnan 1998	To define a methodology to help assess the implementation of self-regulation for the protection of privacy	Translate the FTC principles into a tool that can assess the industry self-regulation effort	Content analysis	A self-regulation checklist. 1.Fair Information Practices (Awareness, choice, data security, data integrity, consumer access, accountability) 2. Enforcement (consumer recourse, verification, consequences)
Smith et al, 1996	To measure the primary dimensions of individuals' concerns about organizational information privacy practices	Organizations' practices of proper handling of customer information	Stage 1: Generate items and assess content validity Stage 2: Instrument testing and selection of items Stage 3: Assess validity and reliability	A 15-item, four-dimension instrument: • Collection • Unauthorized access • Secondary use • Error
Stewart & Segars, 2002	To further develop the Concern For Information Privacy (CFIP) instrument by examining its theoretical meaning, dimensionality, reliability, and validity	Examine the factor structure of the CFIP instrument: • Collection • Unauthoriz-ed access • Secondary use • Error	A survey of 400 consumers in four interview sites	• Each dimension of CFIP is reliable and distinct • CFIP may be more effectively implemented with a higher-order factor structure

Study	Purpose	Focus	Methodology	Key Findings
Sheehan and Hoy, 2000	To apply knowledge of concerns about privacy in traditional direct marketing to the online context, and to assess current FTC policies	The influences on online consumer privacy and its underlying factors	Email survey sent to 3724 people whose email addresses were randomly generated	Three factors underlie consumer concerns about online privacy: • Control of collection and use of information • Short-term, transactional relationships • Established, long-term relationships
Malhotra *et al.* (IUIPC: Internet Users' Information Privacy Concerns), (2002)	To reflect Internet users' concerns about information privacy	Individual awareness of online information privacy issues	Empirical study 1 (instrument development): structured questionnaire, confirmatory factor analysis Empirical study 2 (compare IUIPC & CFIP): developed questionnaires for two types of scenarios – sensitive and insensitive personal information	• Three issues are identified underlying concerns about online privacy: control, knowledge and collection • A ten-item IUIPC instrument is developed • Tests of IUIPC in a conceptual model reveal that particular privacy-related behavior depends highly on context

3.0 Instrument Development

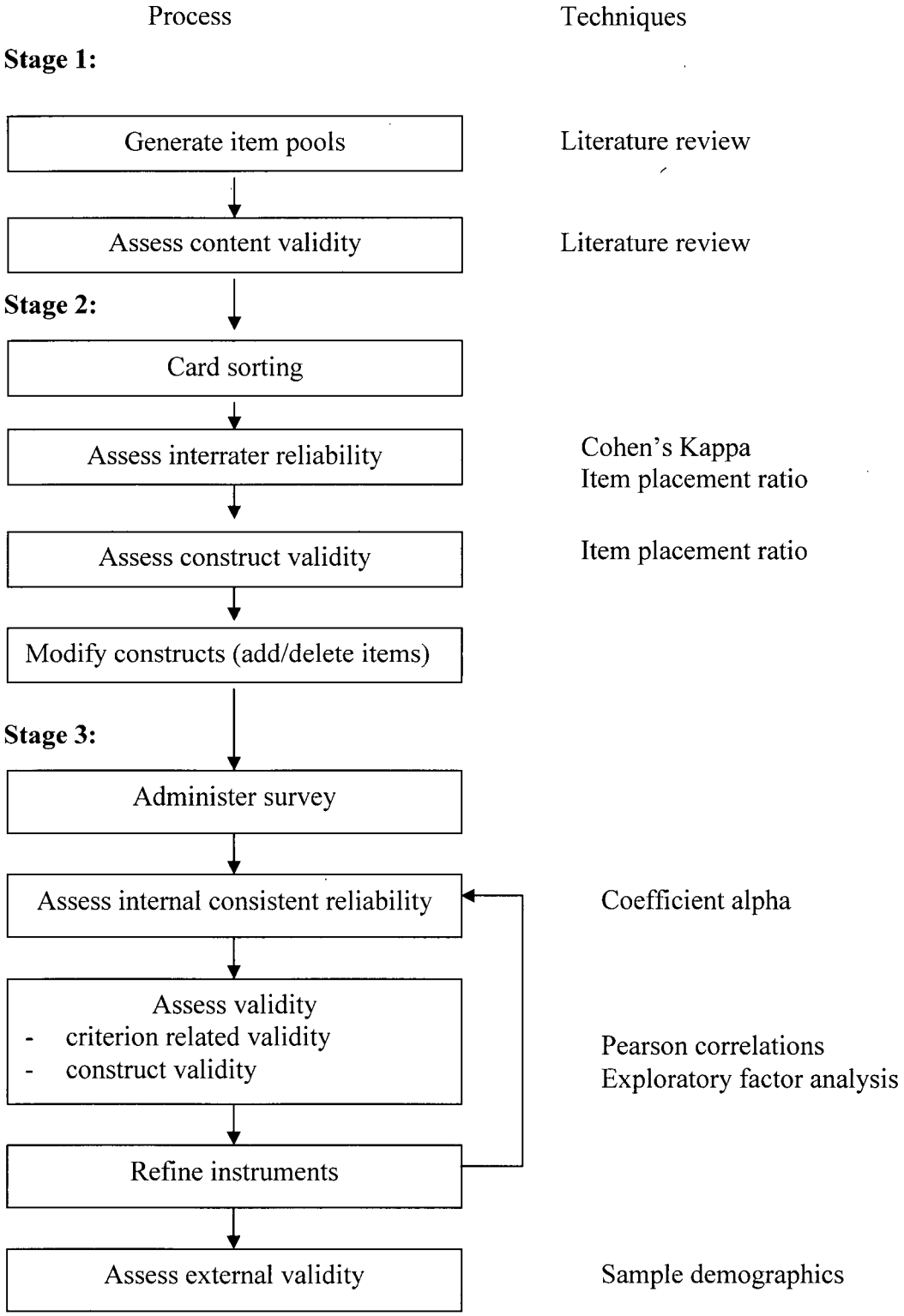
3.1 Methodology Overview

The study focuses on the development of an instrument to measure the degree to which online entities adhere to principles of fair information practices, in the context of consumer perspectives. The instrument development methodology used in Moore and Benbasat (1991) was followed.

There were three stages in the instrument development process. The first was **item creation**. The first stage involved the creation of pools of items for each category based on the FTC's fair information practice principles and the detailed requirements defined in FTC reports. The next stage in the process was **card sorting**. A group of judges sorted the items generated in the first stage into separate categories according to the definitions of a given category. Based on their placements the ambiguous items were deleted from the item pools. The refined scales then went through the **instrument testing** stage as a complete instrument. An online survey was carried out as a field test for the instrument under development.

Figure 2 summarizes the process and techniques used in the instrument development, and the rest of this section describes each stage in detail and the results of data analysis.

Figure 2 Data Collection and Analysis Process and Techniques



3.2 Item Creation

Item pools were generated based on the detailed requirements of the FTC's fair information practice principles (FTC Report to Congress 1998 & 2000). Also referred to were the U.S. Department of Commerce paper, "Element of Effective Self-Regulation for Protection of Privacy" (1998), as well as the questionnaire generated for the Georgetown Internet Privacy Study (Culnan, 1999a) and Culnan's self-regulation checklist (Culnan, 1998). The contents of the Elements paper are almost identical to the FTC's core principles of fair information practice, and some requirements in this document are more specific than the corresponding ones in FTC reports. In Culnan's Georgetown study questionnaire (1999a) and the self-regulation checklist (1998), the detailed requirements of the FTC core principles were translated into coding schemes using content analysis. We reviewed the questions and items in these two documents to ensure that we did not fail to include the relevant principles and requirements in the FTC reports.

In the FTC's 2000 report, "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress", the commission described the widely accepted principles of fair information practices: notice, choice, access and security. The items of the first three categories were newly created based on the detailed description of the corresponding fair information practice principles. Because the content of security principle was similar to the content of "unauthorized access" and "errors" dimensions of CFIP instrument, we adapted the seven items in "unauthorized access" and "errors" for the security category. To ensure the content validity, we reviewed FTC reports from 1998,

1999 and 2000, the Elements paper (US Department of Commerce, 1998), Culnan (1999a) and Culnan (1998) to ensure that we covered all the aspects and requirements of the four principles in developing our instruments (see Table 2).

In this stage 25 items were generated, eight in notice category, six in choice category, four in access category and seven in security category. Table 2 summarizes the items and the sources from which they were created. The items are expressed by various statements in the form of "online organizations should take a certain privacy protection action," and respondents are asked to indicate their level of agreement with the statements, using a seven-point Likert scale ranging from "strongly disagree" to "strongly agree." When wording the item, we use the "comparative degree" (better, more, etc) in most of the statements due to the following reasons:

1. We took into consideration the consistency of item wording across all the constructs. The items in the construct of security are adapted from the constructs of "error" and "unauthorized access" in CFIP and they are worded in this "comparative" way. All other items developed for this study followed the approach.

2. This instrument is designed to capture the "concerns" that, besides measuring individuals' perception about what organizations "should do", we tried to measure their perception about how organizations are "currently doing". For example, if a person strongly agrees that "online companies should have better procedures to XYZ," it implies that the respondent believes that online companies "should take procedures to XYZ" and that the companies "are not currently doing well" in this area.

Table 2 Item List

No.	Items	Source
Notice:		
N1	Online organizations should take more steps to reveal their identity when asking me to give personal information.	FTC (1998) III. A.1. p.7, "identification of the entity collecting the data".
N2	Online organizations should take more steps to disclose how personal information they collect will be used.	FTC (1998) III. A.1. p.7, "identification of the uses to which the data will be put".
N3	Online organizations should take more steps to disclose who will be authorized to access my personal information.	FTC (1998) III. A.1. p.7, "identification of any potential recipients of the data".
N4	Online organizations should take more steps to clearly reveal what personal information they are collecting.	FTC (2000) p. iii, "Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect".
N5	Online organizations should take more steps to clearly reveal the means by which personal information is collected if it is not obvious (e.g., cookies).	FTC (1998) III. A.1. p.8, "the nature of the data collected and the means by which it is collected if not obvious". Georgetown Internet Privacy Policy Survey, Appendix C. p.50, Q26, "Does the site say anything about its use or non-use of Cookies?"
N6 *	Online organizations should have better procedures to notify me as to whether the provision of the personal information they are asking for is voluntary or required.	FTC (1998) III. A.1. p.8 "whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information".
N7 *	Online organizations should take more steps to clearly reveal how they can assure the confidentiality, integrity and quality of the data stored.	FTC (1998) III. A.1. p.8 "the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data".
N8 *	Online organizations should take more steps to clearly reveal our rights with respect to the personal information stored (e.g., accessing to, correcting, and deleting the data.).	FTC (1998) III A.1. p.8, "notice should also identify any available consumer rights, including: any choice respecting the use of the date".
Choice:		
C1	Online organizations should take more steps to get my consent before they collect certain sensitive personal information.	FTC (1998) III A.2. p.8, "Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information;" Department of Commerce (1998), Elements of Effective Self Regulation for the Protection of Privacy, "For certain kinds of information, e.g.,

		medical information ... companies should not use personal information unless its use is explicitly consented to by the individual".
C2	Online organizations should take more steps to get my consent before they use my personal information for certain purposes (e.g., sending targeted email advertising).	FTC (1998) III A.2. p.8, "Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information;" FTC (1998) III A.2. p.9, "choice relates to secondary uses of information ... such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions". Georgetown Internet Privacy Policy Survey, Appendix C. p.50, Q27, "Does the site say that this organization may use information the site has collected to contact consumers for marketing or other purposes?" Q28, "Does the site say that it gives consumers choice about whether they want to be contacted by this organization fro marketing or other purposes?"
C3	Online organizations should take more steps to get my consent before they share personal information with other parties.	FTC (1998) III A.2. p.8, "Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information;" FTC (1998) III A.2. p.9, "choice relates to secondary uses of information ...or external, such as the transfer of information to third parties". Georgetown Internet Privacy Policy Survey, Appendix C. p.51, Q29, "Does the site say that the information collected from consumers may be disclosed to outside third parties?" Q31, "Does the site provide any information about the type(s) or name(s) of the outside third parties to whom the information collected will be disclosed?" Q32, "Does the site say it gives consumers choice about having collected information disclosed to outside third parties?"
C4	Online organizations should have better procedures to allow us to prevent them from collecting certain sensitive personal information.	FTC (1998) III A.2. p.8, "opt-out regimes require affirmative steps to prevent the collection and/or use of such information."
C5	Online organizations should have better procedures to allow us to prevent them from using personal information for certain purposes (e.g., sending targeted email advertising).	FTC (1998) III A.2. p.8, "opt-out regimes require affirmative steps to prevent the collection and/or use of such information." Refer to C2.
C6 *	Online organizations should have better procedures to allow us to prevent them from sharing personal information with other parties.	FTC (1998) III A.2. p.8, "opt-out regimes require affirmative steps to prevent the collection and/or use of such information." Refer to C3.

Access:		
A1	Online organizations should have better procedures to allow us to review at least some of the personal information about us that is stored in their databases.	FTC (2000) p. 17, "The Commission's Survey asked three questions about Access: whether the site says that it allows consumers to (1) review at least some personal information about them; (2) have inaccuracies in at least some personal information about them corrected; and (3) have at least some personal information about them deleted".
A2	Online organizations should have better procedures to allow us to correct at least some of the inaccurate personal information about us that is stored in their databases.	FTC (2000) p. 17, "The Commission's Survey asked three questions about Access: whether the site says that it allows consumers to (1) review at least some personal information about them; (2) have inaccuracies in at least some personal information about them corrected; and (3) have at least some personal information about them deleted".
A3	Online organizations should have better procedures to allow us to delete at least some of the personal information about us that is stored in their databases.	FTC (2000) p. 17, "The Commission's Survey asked three questions about Access: whether the site says that it allows consumers to (1) review at least some personal information about them; (2) have inaccuracies in at least some personal information about them corrected; and (3) have at least some personal information about them deleted".
A4	Online organizations should have better procedures to allow us to contest the accuracy of all personal information about us that is stored in their databases.	FTC (1998) III A.3. p. 9, "It refers to an individual's ability both to access data about him or herself, i.e., to view the data in an entity's files, and to contest that data's accuracy and completeness".
A5 **	Online organizations should have better procedures to allow us to verify the accuracy of my personal information that is shared with other parties.	FTC (2000) p.31, "The Advisory Committee Report also evaluates whether the Access principle should apply to entities other than the original data collector."
Security:		
S1	Online organizations should devote more time and effort to preventing unauthorized access to personal information.	Adapted from CFIP – Unauthorized Access (Smith *et al.* 1996).
S2	Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.	Adapted from CFIP – Unauthorized Access (Smith *et al.* 1996).
S3	Online organizations should take more steps to make sure that unauthorized people cannot access personal information in their computers.	Adapted from CFIP – Unauthorized Access (Smith *et al.* 1996).

S4**	Online organizations should take more steps to ensure the secure transmission of my personal information.	FTC (2000) Appendix B, Q22, "Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide security, for personal information the domain collects, during transmission of the information from the consumer to the domain?"
S5	All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.	Adapted from CFIP – Errors (Smith *et al.* 1996).
S6	Online organizations should take more steps to make sure that the personal information in their files is accurate.	Adapted from CFIP – Errors (Smith *et al.* 1996).
S7	Online organizations should have better procedures to correct errors in personal information.	Adapted from CFIP – Errors (Smith *et al.* 1996).
S8	Online organizations should devote more time and effort to verifying the accuracy of the personal information in their databases.	Adapted from CFIP – Errors (Smith *et al.* 1996).

* Items dropped from scales according to card sorting results
** Items not listed in the card sorting process, but listed in the online survey

3.3 Card Sorting

The goal of this stage is to assess the construct validity of the scales being developed and to further refine the scales by deleting ambiguous or confusing items.

3.3.1 Sorting Procedure

Each item was printed on one index card and the index cards were given to the judges in random order. The judges were also provided with the definitions of the constructs. Before sorting began, the sorting procedure was explained to the judges to ensure that they understood the sorting procedure thoroughly. The judges were also required to read

the construct definitions carefully, and were encouraged to raise any questions, if needed, to fully understand the definitions.

There were eight judges involved in the sorting process. All of them were PhD or Master of Science students in Management Information Systems. After they completely understood the sorting procedure and the construct definitions, the judges were required to sort the 25 index cards into five categories: "notice," "choice," "access," "security" and "too ambiguous/doesn't fit". Each judge finished the card sorting process independently, and did not receive any hint of whether the items were put into "correct" categories. The judges could take as long as they liked to finish the sorting, though on average, the sorting process lasted 15 to 20 minutes.

3.3.2 Sorting Results

3.3.2.1 Interrater Reliability

The reliability of the sorting was assessed using two measurements: Cohen's Kappa and item placement ratio.

Interrater reliability is used to measure the degree of consistency among the raters. Cohen's Kappa establishes how much interrater reliability exists among nominal (i.e. categorical) data. It is designed for situations in which raters classify the items being rated into discrete categories (Huck, 2000, p.94).

In this study, Cohen's Kappa was calculated to assess the interrater reliability of the card sorting results. First, the level of agreement for each pair of judges in item categorization was measured using Cohen's Kappa (see Table 3), and then the level of agreement across all pairs of judges was assessed. There is no general acceptable score for the Kappa, but according to Moore and Benbasat (1991), scores greater than 0.65 are considered acceptable. In this study, the average Kappa score is 0.71, which is higher than the suggested minimum.

Table 3: Cohen's Kappa Scores

	judge 2	judge 3	judge 4	judge 5	judge 6	judge 7	judge 8
judge 1	0.95	0.63	0.67	0.84	0.68	0.84	0.73
judge 2		0.69	0.62	0.89	0.73	0.89	0.68
judge 3			0.36	0.74	0.68	0.74	0.68
judge 4				0.57	0.46	0.57	0.46
judge 5					0.73	0.89	0.68
judge 6						0.84	0.73
judge 7							0.79
Average							**0.71**

Item placement ratio was used to measure the inter-judge agreement. It calculated overall frequency with which the judges put the items in the "correct" category, as shown in Table 4. The higher the percentage of items put in the target construct, the higher the inter-judge agreement in this round of sorting (Moore and Benbasat 1991, p. 201).

There is no determined acceptable level for the placement ratio, but as shown in Table 4, the placement ratios of the notice and choice categories are obviously below the access and security categories, meaning these two categories need to be investigated further.

Table 4: Item Placement Ratio Summary

	Actual Categories						
Target Category	Notice	Choice	Access	Security	Doesn't fit	Total	Target %
Notice	48	4	6	6	0	**64**	**75%**
Choice	1	38	3	4	2	**48**	**79%**
Access	0	1	31	0	0	**32**	**97%**
Security	0	0	2	54	0	**56**	**96%**
Total Item Placements						**200**	
Total Hits						**171**	
Overall Hit Ratio						**86%**	

3.3.2.2 Construct validity

Convergent validity and discriminant validity work together to demonstrate construct validity. Convergent validity refers to a certain correlation of measures of constructs turning out to be high as theoretically predicted, and discriminant validity refers to a certain correlation of measures of constructs being observed to be low as predicted (Huck, 2000, p. 104). An item that is constantly placed into a specific category establishes convergent validity with the related construct and discriminant validity with the others. A category with high "correct" placement ratio can be considered to have a high degree of construct validity. Because the item placement ratios for notice and choice categories are below the ratios of access and security, the items in notice and choice categories should be carefully examined.

As indicated in Moore and Benbasat (1991), the sorting procedure is not strictly quantitative analysis, but rather more qualitative one. There is no established standard to

determine what level of placement ratio is "good" or "acceptable," but the matrix may be a reflection of any potential problem areas.

Table 5 Placement Ratio by Item

Target Category	Item No.*	Actual Categories: Notice	Choice	Access	Security	N/A	Total	Hit rate
Notice	N1	7			1		8	87.5%
	N2	8					8	100.0%
	N3	6		1	1		8	75.0%
	N4	8					8	100.0%
	N5	8					8	100.0%
	N6	4	3		1		8	***50.0%***
	N7	5			3		8	***62.5%***
	N8	2	1	5			8	***25.0%***
Choice	C1		7			1	8	87.5%
	C2	1	6	1			8	75.0%
	C3		7	1			8	87.5%
	C4		6	1		1	8	75.0%
	C5		7		1		8	87.5%
	C6		5		3		8	***62.5%***
Access	A1			8			8	100.0%
	A2			8			8	100.0%
	A3		1	7			8	87.5%
	A4			8			8	100.0%
Security	S1				8		8	100.0%
	S2			1	7		8	87.5%
	S3				8		8	100.0%
	S4				8		8	100.0%
	S5				8		8	100.0%
	S6			1	7		8	87.5%
	S7				8		8	100.0%
Total hits:							**200**	

* Please refer to Table 2 for item details.

We calculated the "hit rate" of each item according to the card sorting results. The "hit rate" represents the percentage of times the item is placed in the target category. The results showed that three items in the notice category and one item in the choice category

were confusing. There was a high possibility that they were put into a category other than the one targeted. After examining how the deletion of these items would affect the content validity, we found that they were covered in other constructs or items: the content of the other items in the choice category cover N6 and C6, the items in the access category cover N8 and the items in the security category cover N7. As a result, these four confusing items were deleted from the scales without damaging the content validity. Table 5 summarizes the item placement status as the result of the card sorting process.

3.4 Instrument testing

3.4.1 Survey administration

An online survey was conducted to test the instruments being developed. Data were collected between August 13 and August 24, 2003, using a questionnaire with three sections (see Appendix 2). Section one contained Likert-scale questions covering the whole instrument under development, CFIP instrument and other consumer trust measurements. Using the card sorting results, we deleted four items from the original 25-item instrument and created one additional item for the access category and one for the security category. Therefore, for the instruments being tested in this survey there were 23 questions in total: five items each in the notice, choice and access categories and eight in the security category. The questionnaire did not set up any specific scenarios or context when asking the respondents' perceptions of privacy issues. Their perceptions of online privacy concerns in general were solicited. Section two contained nine questions to

measure consumers' attitudes and intentions towards giving out personal information. Section three contained seven questions about the respondents demographic and Internet usage information. The questionnaire is enclosed as Appendix 2.

An online research company located in California, U.S. was hired to run the survey. The company sent out emails to its panel members to invite them to participate in the survey. In order to prevent multiple responses from one respondent the company sent out a unique identification number in each survey invitation, which was required in the survey response. The interested members logged on to the survey web site and completed the questionnaire online. For each response, the submitted time and IP address were recorded in order to avoid redundancy.

3.4.2 Sample

The target subjects of this survey were Internet users. Most of them were from U.S. since we hired a U.S. company to run the survey. There were 563 responses collected from the online survey between August 13 and August 24, 2003. We do not have the accurate response rate since the research company did not provide us the number of invitation letters they sent out for this survey. According to their experience, they typically get a 20% response rate.

Table 6 Respondent Profile (n=376)

Demographic Characteristic		Percentage of Respondents
Gender	Male	30.6%
	Female	69.4%
Education	Some school, no degree	2.2%
	High school graduate	15.9%
	Some college, no degree	44.6%
	Bachelors' degree	24.2%
	Master's degree	9.1%
	Professional degree	3.5%
	Doctoral degree	0.5%
Purchase anything from Internet?	Yes	91.1%
	No	8.9%
Internet access frequency	Never	0.5%
	Less than once per week	17.9%
	1-2 times/ week	19.5%
	3-4 times/ week	20.0%
	5-6 times/ week	9.6%
	7-10 times/ week	14.4%
	10-20 times/ week	5.9%
	more than 20 times per week	12.3%
Online purchase frequency	Never	7.8%
	Less than once per month	47.1%
	1-5 times/ month	38.8%
	6-15 times/ month	4.5%
	16-20 times/ month	1.3%
	21-30 times/ month	0.5%
Online purchase amount in past 6 months	None	8.8%
	$1 - $49	15.2%
	$50 - $99	16.0%
	$100 - $199	12.8%
	$200 - $499	24.3%
	$500 - $999	10.4%
	$1000 - $1999	8.0%
	$2000 - $3999	2.7%
	$4000 - $9999	1.9%

Others		
Age	Range	18-63
	percentile 25	25
	50	33
	75	46

The responses with missing data were screened out and 493 complete responses remained. Two responses with unreasonable data ("3" or "99" appeared in the "age" field) were also screened out. Responses submitted with the same IP address more than three times were eliminated. We allowed the same IP address to appear three or less because it was possible that family members shared one computer or one IP address at home. We received 376 valid responses.

Table 6 reports the demographic and Internet usage profile of the 376 respondents. Approximately 70% of the respondents were female, 50% were between the ages of 25 and 46, and 37.3% had earned a Bachelor's degree or higher. 91% had online purchase experience, 45% purchase online more than once per month, and 91% had spent money on Internet purchase in the past six months. 82% of the respondents were active Internet users, accessing the Internet at least once per week.

3.4.3 Results

3.4.3.1 Internal Consistency Reliability

As a first step, data internal consistency reliability was assessed. Internal consistency reliability is defined as consistency across the parts of a measuring instrument. Coefficient alpha (Cronbach's alpha) can be used with instruments made up of items that

can be scored with three or more possible values, such as a Likert-type questionnaire. Table 7 reports the analysis of coefficient alpha. The alphas are all over 0.9, indicating that the scales have sufficient homogeneity.

Table 7: Reliability Coefficient – Coefficient Alpha (four constructs)

Scale name	Number of items	Alpha
Notice	5	0.93
Choice	5	0.95
Access	5	0.95
Security	8	0.94

3.4.3.2 Criterion-related Validity

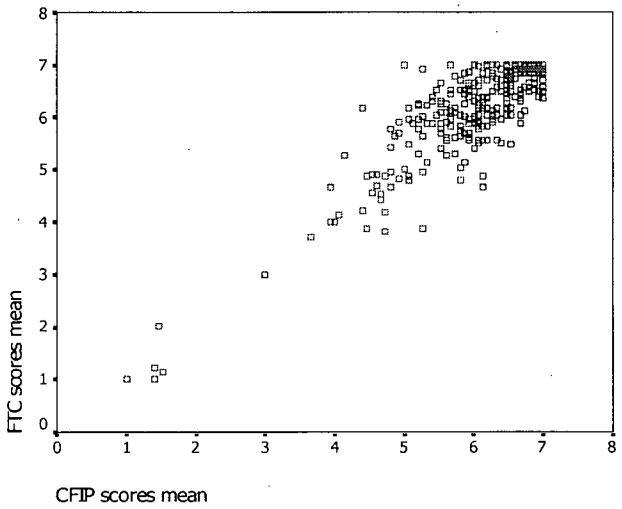
Criterion-related validity is used to assess the accuracy of the new instrument by comparing scores from the new instrument with scores on a relevant criterion variable, which has been demonstrated valid (Huck, 2000, p.101). The validity will be determined by (1) determining how various people perform on the new test and on the criterion variable, and (2) correlating these two sets of scores. The CFIP instrument has existed since 1996, has been used in consumer privacy concerns studies for many years, and is an appropriate candidate for the "relevant criterion variable." We collected data for the new instrument and the CFIP instrument scores in the same online survey, hence investigated the concurrent validity. To test the correlation of these two sets of scores, we averaged all items in each instrument respectively and correlated the two sets of means. The scatter diagram (see Figure 3) implies a high-high, low-low relationship between these two sets of scores. The correlation coefficient of the samples is high (0.9), indicating that the two constructs are highly correlated, which demonstrates the high criterion-related validity of the new instruments.

Table 8: Criterion-related Validity – Correlation Coefficient

	FTC mean	CFIP mean
Mean	6.29	6.17
Std. Deviation	0.99	0.96
Pearson Correlation	0.90*	

*Correlation is significant at 0.01 level (2 tailed).

Figure 3 Scatter Diagram of the means of FTC scores and CFIP scores



The scatter diagram also implies a threat of ceiling effects, which is that we cannot compare the two methods well because both are achieving near the best practicable. In Figure 3 we can see that most of the spots located in the area between 6 and 7. Ceiling effects may affect the result of criterion-related validity assessment.

3.4.3.3 Construct Validity

Factor analysis was used to assess the construct validity of the instruments being developed. We performed a principal components analysis with a Promax rotation. In step

1, we loaded items within each category. Because each category was developed based on one concept, one factor was expected to be extracted in each category, which would demonstrate convergent validity in the scales. In step 2, we loaded all items of the instruments to confirm the results from step 1 and test the discriminant validity of the scales.

Step 1. Factor Analysis with Items for Each Category.

Principle component extraction with Promax (Oblique) rotation was conducted upon items within each category. According to the eigenvalues (the Kaiser criterion) and the scree scores, one factor was extracted from each of three categories: notice, choice and access. The results of the factor extraction shown in Table 9 demonstrate the convergent validity of these three scales. Two factors emerged from the security category: item S1 to S4 belong to the first factor, and S5 to S8 belong to the second factor. From the correlation matrix (Appendix 3) we can also see that the inter-item correlation scores between items S1-S4 and items S5-S8 are notably lower than the scores within S1-S4 and S5-S8. In fact, since we adapted S1 - S3 from "unauthorized access" and S5– S8 from "errors" of CFIP instrument (S4 was newly created), we can explain the justification of the two factors extracted from security.

Table 9 Summary of Eigenvalues – Principle Components Extracted by Category (n=376)

		Eigenvalue	
Category	Number of items	Component 1	Component 2
Notice	5	3.932	0.371
Choice	5	4.185	0.295
Access	5	4.211	0.302
Security	8	5.704	1.064

Step 2. Factor Analysis with all the Items.

In step 2, we conducted a principle components analysis with Promax rotation, specifying a five-factor solution to all 23 items. The reasons we pre-specify a five-factor solution in the factor extraction are as follows:

1. In step 1 we totally extracted five factors: one from notice, choice and access and two from security.

2. The Kaiser criterion, specifying the eigenvalues that are greater than 1 (E1 rule), is the most commonly used criterion for deciding how many factors to extract. Many previous studies on privacy concerns or instrument developments also used this criterion in their factor analysis. However, as indicated in Richardson & Fico (2003), "no consensus has emerged on universally applicable rules for deciding how many factors to retain. However, there does appear to be a consensus that of all criteria proposed, the E1 rule is among the very worst" (Richardson and Fico 2003, p. 12). This study also suggested that there were no "universally applicable rules" to decide the number of factors, and that the researchers' judgement based on the underlying theory might be the best method. We developed the four constructs based on four different concepts and the security scale was adapted from two different constructs of CFIP instrument, so it is appropriate to assume that there are five factors underlying these 23 items.

In this study we use Promax rotation, instead of the Varimax rotation commonly used in other instrument development studies. There are two main types of rotation in factor extraction: orthogonal and oblique. Orthogonal rotation imposes the condition on the data that all factors must be uncorrelated. There is no condition for the oblique rotation (Richardson & Fico, 2003). In our study, each of the four constructs in the instruments is developed to measure the consumer perceptions of online entities' information practices, and all are based on the four FTC fair information practice principles. Furthermore, as indicated in the FTC's 1998 report, the principles of choice and access were only meaningful when the principle of notice was implemented. Based on these facts we assumed that the factors were highly correlated, and we chose Promax rotation - one of oblique rotations - in our factor extraction. In fact, the analysis later demonstrated that the inter-factor correlations for the five factors ranged from 0.338 to 0.703, when applying factor analysis to the whole sample.

To confirm the five-factor assumption we conducted a principle components analysis with Promax rotation, specifying a five-factor solution to all 23 items. These five factors captured 84% of the variance, and a simple factor structure emerged. From the matrix (Table 10) we can see that no item loaded on more than one factor. As expected, all items loaded together on the target factors. According to the factor loading standards indicated in Comrey (1973), 19 out of 23 remaining items loaded on the target factors in the "excellent" range (over 0.71), three items loaded in the "very good" range (0.63 – 0.71), and one item in the "good" range (0.55 – 0.63).

Table 10 Pre-specified five- factor solution (n=376)

Total Variance Explained

	Initial Eigenvalues		
Component	Total	% of Variance	Cumulative %
1	15.137	65.812	65.812
2	1.679	7.299	73.111
3	.965	4.195	77.306
4	.861	3.744	81.050
5	.614	2.670	83.720

Pattern Matrix

	Component 1	Component 2	Component 3	Component 4	Component 5
Notice item 1	0.818	0.084	0.077	-0.094	-0.022
Notice item 2	0.885	-0.099	-0.017	-0.031	0.161
Notice item 3	0.814	-0.028	-0.038	0.027	0.163
Notice item 4	0.873	0.080	-0.033	0.104	-0.112
Notice item 5	0.749	0.168	0.093	-0.023	-0.057
Choice item 1	0.167	0.793	0.097	0.053	-0.194
Choice item 2	0.041	0.925	-0.056	0.001	0.025
Choice item 3	0.000	0.887	-0.048	-0.048	0.139
Choice item 4	0.011	0.784	-0.017	0.105	0.074
Choice item 5	0.006	0.738	0.099	-0.064	0.202
Access item 1	0.103	-0.086	0.861	0.002	0.051
Access item 2	0.007	0.009	0.938	0.081	-0.102
Access item 3	-0.037	-0.076	0.840	-0.039	0.206
Access item 4	0.006	0.101	0.860	0.057	-0.058
Access item 5	0.000	0.124	0.794	-0.003	0.060
security item 1	-0.008	0.275	0.115	0.023	0.602
security item 2	0.074	-0.074	-0.040	0.122	0.863
security item 3	0.003	0.235	0.087	-0.018	0.696
security item 4	0.055	0.201	0.048	-0.002	0.696
security item 5	0.057	-0.193	-0.035	0.803	0.293
security item 6	-0.003	0.028	-0.040	0.927	0.060
security item 7	0.053	0.083	0.259	0.663	-0.078
security item 8	-0.079	0.104	0.017	0.967	-0.098

Extraction Method: Principal Component Analysis. Rotation Method: Promax with Kaiser Normalization.

Because two factors were extracted from the original construct of security, and the FTC principle of security contains two aspects - data security and accuracy/integrity - we named the first factor which includes the first four items; "security." The second factor, containing S5-S8, was named "integrity". The finalized FTC constructs are listed as Appendix 4.

The scales may still be improved. As seen in Table 11, all five scales achieve a rather high level of reliability scores (all Alphas are over 0.9). According to DeVellis (1991), alphas between 0.8 and 0.9 fall in the "very good" range. If alpha is much higher than 0.9, the scale can be considered to be shortened (DeVellis 1991, p.85). However, in this study, after reviewing the contents of the five scales and considering the factor analysis results, we did not delete any items from the scales because of content validity. We include the inter-item correlations for all scales in Appendix 5, and the means and standard deviations by item in Appendix 6. They can help to guide the deletion of any items from the scales in the future.

Table 11: Reliability Coefficient – Coefficient Alpha (five constructs)

Scale name	Number of items	Alpha
Notice	5	0.93
Choice	5	0.95
Access	5	0.95
Security	4	0.94
Integrity	4	0.93

4.0 Discussion and Conclusion

4.1 Discussion

Through the process described in chapter 3, we developed an instrument to measure online consumers' perceptions of privacy practices based on the FTC fair information practice principles. First, we generated 25 items based on the definitions and requirements of the four fair information principles. Secondly, these 25 items went through a card sorting process, and according to the card sorting results, we deleted four confusing items from the scales and added two items. Third, we carried on an online survey for instrument testing. After applying factor analysis to the survey data we were left with five factors from the 23 items, instead of four as we first expected. And the results of other validity and reliability analyses demonstrated that the newly developed instrument demonstrates sufficient validity and reliability. Finally, we produced a five- construct, 23- item FTC instrument. The five constructs are notice (5 items), choice (4 items), access (5 items), security (4 items) and integrity (4 items). All items in the first three constructs are newly created according to the requirements of the FTC fair information practice principles, and construct security and integrity are adapted from CFIP instrument.

Table 12 Comparison of the FTC instrument's Five Factors with the Corresponding Dimensions of Privacy Concerns in Previous Studies

Study	FTC instrument	CFIP	Sheehan & Hoy	IUIPC
Related factors / dimensions	Notice		Control of collection and use of information	Knowledge
	Choice	Secondary use	Control of collection and use of information	Control
	Access			
	Security	Unauthorized access		Collection
	Integrity	Error		
		Collection		
			Short-term, transactional relationships	
			Established, long-term relationships	

Table 12 summarizes the relationships among the FTC instrument's five factors and the dimensions of online privacy concern in previous instruments and studies. The factors and dimensions are considered to be "related" only because they cover the same aspect of the information privacy concern. It is not necessary that they are exactly identical in content or definition.

As mentioned in the first chapter, both the CFIP instrument and the FTC instrument can be used to measure the individuals' perception for organizations' information privacy practices. However, the CFIP instrument was developed before the Internet was popular and did not take into account the numerous interfaces between consumers and organizations. From Table 12 we can see the aspects of privacy concerns that the CFIP

instrument fails to cover:

1. There is no directly relevant factor in the FTC instrument for the "collection" dimension of CFIP. The "collection" refers to the concerns that extensive amount of personal information are collected and stored. However, the FTC principle of notice requires that the consumers should be informed in advance what kind of personal information will be collected and how the personal information will be used. And if the principle of choice is followed, the online consumers should have right to prevent the collection of their personal information and control the usage. These two factors will help relieve the consumer's concern that too much personal information is being collected, because the two way communications between consumers and companies provide consumers with more control over the collection and usage of their personal information.

2. There is no relevant dimension of CFIP relating to the "notice" and "access" in the FTC instrument. "Notice" requires that online organizations should inform consumers about their information practices before they collect any personal information. "Access" refers to the consumers' ability to access, correct or delete their own personal information stored by online companies. In the offline environment it is not feasible for the organizations to take such actions. Therefore, such factors are not included in the CFIP instrument.

3. We adapted three out of four items of the 'security" construct from the "unauthorized access" construct of CFIP. The newly created one is about the concern of secure

transmission of personal information. Internet makes the transmission of information much easier and more frequent, also raises the security concern of the transmission of personal information.

Previous studies indicated that the online privacy concerns were highly contextual (Sheehan & Hoy 2000, Malhotra et al 2003). The results of the privacy concerns study (Phelps, Nowak and Ferrell 2000) in the conventional context (offline) showed that the type of personal information requested was one of the important correlates of privacy concern. The online environment adds to the contextual nature of privacy concerns due to the ease with which an online user can change to, or happen upon, a new online entity. Among the previous studies referred to in this study, there is no contextual setting involved in the CFIP development in the work of either Smith et al (1996) or Stewart & Segars (2002). When Malhotra et al (2003) developed IUIPC, they defined the information privacy concerns without accounting for situations or contexts. However, in the empirical study that compares IUIPC and CFIP and tests the structural model after the instrument development, they applied two scenarios (sensitive and insensitive information collection) in the survey. In Sheehan & Hoy survey (2000) they included scenarios presenting three different levels of predicted privacy concern in order to capture the contextual nature of privacy and the online environment.

However, no specific scenarios/situations were included in the development process in this study due to the following reasons:

1. The new instrument was not developed for the measurement of any particular industries or web sites. The goal was to develop an instrument to measure the information practices of online entities that collect personal information regardless of the nature of their business, the type of information they request, the usage of the personal information they collected, and other similar factors.

2. The new instrument was developed based on the four FTC fair information practice principles. The definitions of the FTC principles were set forth to be broad enough to provide flexibility in implementation, because the FTC recognized that the implementation of fair information practices might need to adapt to the nature of the information collected, the use of the information, and the development of the technologies.

4.2 Implications

The contribution of this study is a validated instrument for measuring individual's perception of online privacy practices. Using this instrument, researchers can measure an individual's privacy concerns regarding online marketers' information practices, and then further examine the relationships between privacy concerns, privacy-related variables, outcomes of privacy concerns, privacy concerns' influences, and other factors. By comparing the results of the FTC instrument and other online privacy concern measurements researchers may identify limitations of the current FTC principles from an academic research point of view.

Online companies and web sites can use this instrument to evaluate their own consumer privacy protection policies and mechanisms. They can assess whether their information practices provide sufficient protection to consumers from the consumers' point of view. They can also identify underlying privacy-related problems and take corrective actions to relieve potential consumers' privacy concerns, which may be an obstacle to online sales.

The FTC's core principles were summarized from several decades government reports, guidelines and model codes related to information practices (FTC 1998, p. 7). Previous FTC studies of online privacy focused on the assessment of the industry's self-regulation progress. These reports and surveys used content analysis to study online privacy protection from the marketers' point of view. The newly developed FTC instrument can help public policy makers better understand online consumer privacy concerns from the perspective of consumers.

There are two main benefits for online buyers. First, they can gain more knowledge about their privacy rights with the use of the instrument. Some respondents commented that our survey was "informative" and made them "think more about their privacy rights." Second, they can use the instrument as a tool to evaluate a web site's information practices and judge whether the practices and privacy protection mechanisms are fair and adequate, and whether their privacy rights are properly protected. When online consumers gain sufficient information about their privacy rights and have practical measures to access online privacy protection practices, they may have fewer concerns about privacy issues and indulge more frequently in e-commerce.

4.3 Limitations

There are some limitations in this study. The first is a threat to the study's external validity. External validity is the degree to which the conclusions in the study can be generalized. In the instrument testing stage, we hired a marketing research company to run the survey for us. The research company is located in the United States. After comparing our respondent profile with the online buyer profile and Internet user profile (see Table 13), we found that although 90% of our respondents had online shopping experience and over 80% were active Internet users, there were still differences in the demographic data (e.g. age and gender). This may affect the external validity of the study.

Table 13 Internet Users Profile

Respondent profile	American online buyer profile (Ernst & Young, 2000)	US Online Adults profile 2001 (summarized by Internet Studio, Inc)
Age 18-34 – 55% Age 35-54 - 31% Age 55+ - 14% Median age is 33 37% have bachelor's degree or above 30% are male	Median age is 41 41% graduate from college 50% are male	Age 18-34 - 39% Age 35-54 - 47% Age 55+ - 14% 49% are male

In addition to the demographic differences between our sample and the online user profile, we have some concern for our sample's tendency towards privacy concerns. Our respondents are members of an online research firm and there is a possibility that they are inclined to have fewer concerns for privacy than other Internet users. This may also affect the representativeness of our sample.

As discussed in section 4.1, we developed and validated the FTC instrument without any context in consideration. Therefore, when applying our instrument to a specific context, e.g. use it to measure a particular web site, there may be a threat to the validity and reliability of the constructs. Reassessment of the construct validity and reliability is suggested when adapting the FTC instrument into a context specific situation.

4.4 Conclusion and suggestions for future study

The purpose of this study is to develop an instrument to measure the degree to which online entities adhere to fair information practice principles, from the consumers' perspective. In developing this instrument, we followed the development methodology used in Moore and Benbasat (1991). The process included three stages: item creation, card sorting, and instrument testing. In the first stage we generated 25 items based on the definitions of the four fair information principles. In the second stage, we asked eight judges to sort the 25 items into various categories, and according to the card sorting results we deleted four confusing items from the scales and added two items. In the third stage, we conducted an online survey to test the instruments. Over 500 responses were collected online, 376 of which were usable. We then applied reliability and validity analyses to the data .The results demonstrated acceptable reliability and validity level for the instrument under development. We believe that the method of developing the instruments provided sufficient confidence in the content and construct validity.

The result is a 23-item instrument, including five scales, all with an acceptable level of

reliability. This instrument can be used to evaluate the privacy protection practices of online entities and judge whether these practices are fair and provide sufficient protection to consumers.

We did not compare the explanatory or predictive power of the new instrument with the power of other instruments measuring online privacy concerns, such as CFIP, in a nomological framework. To place the FTC instrument into a context-specific nomological framework and compare it with other instruments may be an opportunity to further develop the FTC instrument.

The instrument was developed based on the current definitions of the FTC's fair information practice principles. Some previous studies, such as Sheehan and Hoy (2000), suggested that certain dimensions or principles (i.e. "the issue of exchange") might be suitable to add to the FTC core principles. With the expansion of e-commerce, fast-developing technology, and increasing privacy concerns among online consumers, the Federal Trade Commission may be in need of updating its core principles or guidelines to adapt to the changes that have occurred, and will continue to occur, in the online environment. In such circumstances, the instrument created in this study may need to be refined according to changes in the core principles of fair information practice.

BIBLIOGRAPHY

Chin, Wynne W., Abhijit Gopal, and W. David Salisbury (1997), "Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation," *Information Systems Research*, Vol. 8 Issue. 4, 342-67.

Comrey, A.L. (1973), "A First Course in Factor Analysis." *Academic Press*, New York.

Culnan, Mary J. (1998), "A Methodology to Assess the Implementation of the Elements of Effective Self-Regulation for Protection for Privacy," available at <http://www.msb.edu/faculty/culnanm/Privacy/NTIA.pdf>

Culnan, Mary J. (1999a), "Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission," available at <http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.PDF>

Culnan, Mary J. (2000), "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing*, Spring 2000, Vol. 19 Issue. 1, 20-26.

Culnan, Mary J. and Armstrong, Pamela K. (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, Vol.10, Issue. 1, Jan.-Feb. 1999.

Devellis, Robert F. (1991), "Scale development: Theory and applications", *Sage,* Newbury Park, California.

Ernest & Young (2000), "Online Demographics," available at <http://www.onemerchant.com/marketing demographics.pdf>

Forrester Research (2000), *Forrester Privacy Best Practice Report*, cited in Microsoft Advertisement, N.Y. Times, Mar. 23, 2000, A12.

Hoffman, Donna L. and Thomas P. Novak (1996), "Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations," *Journal of Marketing*, 60 (July), 50-68

Huck, Schuyler W. (2000), "Reading Statistics and Research", *Addison Wesley Longman, Inc,* 3rd edition.

Internet Studio, Inc, "Who is online?" available at: <http://www.theistudio.com/whois_online.html>

Jupiter Communications, Inc. (1999), *Overview: Proactive Online Privacy: Scripting an Informed Dialogue to Allay Consumers' Fears*, available at <http://www.jup.com>

Malhotra, Naresh K., Kim, Sung S. and Agarwal, James (2002), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Nomological Framework," working paper available upon request <http://instruction.bus.wisc.edu/skim/vita/>

Milne, George R. and Gordon Mary Ellen (1993), "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework," *Journal of Public Policy & Marketing,* Vol.12 Issue.2, Fall 1993, 206-215.

Miyazaki, Anthony D. and Fernandez, Ana (2000), "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing*, Spring 2000, Vol. 19 Issue 1, 54-61.

Moore, Gary C. and Benbasat, Izak (1991), "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research*, September 1991, Vol. 2 Issue 3, 192-222.

Phelps, Joseph, Nowak, Glen and Ferrell, Elizabeth(2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information", *Journal of Public Policy & Marketing*, Spring 2000, Vol. 19 Issue 1, 27-41.

Richardson, John D. and Fico, Frederick (2003), "Do Mass Communication Studies Test Measures for Unidimensionality?" *paper presented at the annual meeting of the Association for Education in Journalism and Mass Communication, Kansas City, MO* July 2003, available at: <http://www.msu.edu/~richa377/Papers_Presented.htm>

Sheehan, Kim Bartel and Hoy, Mariea Grubbs (2000), "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, Spring 2000, Vol. 19 Issue 1, 62-73.

Smith, H. Jeff; Milberg, Sandra J. and Burke Sandra J. (1996), "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly*, Jun 1996, Vol. 20 Issue 2, 167-196.

Stewart, Kathy A. and Segars, Albert H. (2002), "An Empirical Examination of the Concern for Information Privacy Instrument", *Information Systems Research*, Mar. 2002, Vol. 13 Issue 1, 36-49.

United States Department of Commerce, National Telecommunications and Information Administration, "Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy", available at <www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm>

United States Department of Commerce, "2001 E-commerce Multi-sector Report", available at <http://www.census.gov/eos/www/ebusiness614.htm>

United States Federal Trade Commission (1998), "Privacy Online: A Report to Congress," available at <http://www.ftc.gov/reports/privacy3/index.htm>

United States Federal Trade Commission (1999), "Self-Regulation and Privacy Online: A Report to Congress," available at < http://www.ftc.gov/os/1999/07/index.htm#13>

United States Federal Trade Commission (2000), "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress," available at <http://www.ftc.gov/os/2000/05/index.htm#22>

William M. Trochim, "Research Methods Knowledge Base", *Cornell University,* <available at http://trochim.human.cornell.edu/kb/>

Appendix 1 Concern for Information Privacy (CFIP) Constructs

Collection:

1. It usually bothers me when companies ask me for personal information.
2. When companies ask me for personal information, I sometimes think twice before providing it.
3. It bothers me to give personal information to so many companies.
4. I'm concerned that companies are collecting too much personal information about me.

Errors:

1. All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.
2. Companies should take more steps to make sure that the personal information in their files is accurate.
3. Companies should have better procedures to correct errors in personal information.
4. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Secondary Use:

1. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided information.
2. When people give personal information to company for some reason, the company should never use the information for any other reason.
3. Companies should never sell the personal information in their computer databases to other companies.
4. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Unauthorized Access:

1. Companies should devote more time and effort to preventing unauthorized access to personal information.
2. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
3. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

Appendix 2: Online Survey Questionnaire

Online Privacy Survey

Notes:

It should take about 15 minutes to complete this survey. Your answers will be kept strictly confidential and used only for analyses to accomplish the objective of this study. We would also like to assure you that individuals will never be identified and analyses will be conducted only at the aggregate level.

As you go through the questionnaire, you may feel that some of the questions appear to be repetitious. These are not meant to be trick questions.

SECTION 1 (Likert-Scale Questions)

Based on your personal views about ***how online companies are currently dealing with your personal information***, please indicate the extent to which you agree or disagree with each statement.

1. Online companies should take more steps to reveal their identity when asking me to give personal information.
2. Online companies should take more steps to disclose how personal information they collect will be used.
3. Online companies should take more steps to disclose who will be authorized to access to my personal information

1. Online companies should take more steps to clearly reveal what personal information they are collecting.
2. Online companies should take more steps to clearly reveal the means by which personal information is collected if it is not obvious (e.g., cookies).
3. Online companies should take more steps to get my consent before they collect certain sensitive personal information.
4. Online companies should take more steps to get my consent before they use my personal information for certain purposes (e.g., sending targeted email advertising).
5. Online companies should take more steps to get my consent before they share personal information with other parties.
6. Online companies should have better procedures to allow us to prevent them from collecting certain sensitive personal information.
7. Online companies should have better procedures to allow us to prevent them from using personal information for certain purposes (e.g., sending targeted email advertising).
8. Online companies should have better procedures to allow us to review at least some of the personal information about us that is stored in their databases.
9. Online companies should have better procedures to allow us to correct at least some of the inaccurate personal information about us that is stored in their databases.
10. Online companies should have better procedures to allow us to delete at least some of the personal information about us that is stored in their databases.
11. Online companies should have better procedures to allow us to contest the accuracy of all personal information about us that is stored in their databases.

Appendix 2 (continued)

12. Online organizations should have better procedures to allow us to verify the accuracy of my personal information that is shared with other parties.
13. Online companies should devote more time and effort to preventing unauthorized access to personal information.
14. Computer databases that contain personal information should be protected from unauthorized access-no matter how much it costs.
15. Online companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
16. Online organizations should take more steps to ensure secure transmissions of my personal information.
17. All the personal information in computer databases should be double-checked for accuracy-no matter how much this costs.
18. Online companies should take more steps to make sure that the personal information in their files is accurate.
19. Online companies should have better procedures to correct errors in personal information.
20. Online companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
21. It usually bothers me when online companies ask me for personal information.
22. When online companies ask me for personal information, I sometimes think twice before providing it.
23. It bothers me to give personal information to so many online companies.
24. I'm concerned that online companies are collecting too much personal information about me.
25. Online companies should not use personal information for any purpose unless it has been authorized by the individuals who provided information.
26. When people give personal information to an online company for some reason, the online company should never use the information for any other reason.
27. Online companies should never sell the personal information in their computer databases to other companies.
28. Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Appendix 2 (continued)

SECTION 2:

The following statements describe ***your attitudes and intentions toward giving personal information to online companies***. Please indicate the extent to which you agree or disagree with each statement.

Providing personal information to online companies is:

1. Bad idea	___	___	___	___	___	___	___ Good idea
2. Unfavorable	___	___	___	___	___	___	___ Favorable
3. Wise	___	___	___	___	___	___	___ Foolish
4. Positive	___	___	___	___	___	___	___ Negative
5. Attractive	___	___	___	___	___	___	___ Unattractive

Given a chance in the near future, specify the extent to which you would give personal information to online companies

1. Unlikely	___	___	___	___	___	___	___ Likely
2. Not probable	___	___	___	___	___	___	___ Probable
3. Possible	___	___	___	___	___	___	___ Impossible
4. Willing	___	___	___	___	___	___	___ Unwilling

SECTION 3: Demographic and Other Information

Please answer the following questions regarding your demographic information and Internet usage.

1. Your gender: __ Male __ Female
2. Your age: __ years old
3. Education level:
   - Some school, no degree
   - High school graduate
   - Some college, no degree
   - Bachelor's degree
   - Master's degree
   - Professional degree
   - Doctorate degree
4. Have you purchased any products from the Internet so far?

Yes No

Appendix 2 (continued)

5. On average, how often do you casually browse or search for any product/service offerings through the Internet?

Never

- Less than once per week
- 1-2 times / week
- 3-4 times / week
- 5-6 times / week
- 7-10 times / week
- 11-20 times / week
- More than 20 times / week

6. On average, how often do you make online purchases of any products from online retailers?

- Never
- Less than once a month
- 1-5 times / month
- 6-15 times / month
- 16-20 times / month
- 21-30 times / month
- More than 30 times / month

7. What is the TOTAL amount you spent to purchase any products through the Internet during the past 6 months?

- None
- $1 - $49
- $50 - $99
- $100 - $199
- $200 - $499
- $500 - $999
- $1000 - $1999

- $2000 - $3999
- $4000 - $9999
- more than $10,000

8. Please enter your User ID (Required, found at the top of the email invitation)

9. Any comments or suggestions on this survey?

Appendix 3: Inter-item correlation matrix – Security

	S1	S2	S3	S4	S5	S6	S7	S8
S1	1.0000							
S2	.7407	1.0000						
S3	.8772	.7540	1.0000					
S4	.8340	.7849	.8539	1.0000				
S5	.6021	.6063	.5943	.5439	1.0000			
S6	.5982	.6071	.5776	.6057	.7840	1.0000		
S7	.6551	.5562	.6459	.6035	.6993	.7956	1.0000	
S8	.5325	.5333	.5145	.5403	.7333	.8635	.7653	1.0000

N of Cases = 376.0

Appendix 4 FTC constructs

Notice:

1. Online organizations should take more steps to reveal their identity when asking me to give personal information.

2. Online organizations should take more steps to disclose how personal information they collect will be used.

3. Online organizations should take more steps to disclose who will be authorized to access my personal information.

4. Online organizations should take more steps to clearly reveal what personal information they are collecting.

5. Online organizations should take more steps to clearly reveal the means by which personal information is collected if it is not obvious (e.g., cookies).

Choice:

1. Online organizations should take more steps to get my consent before they collect certain sensitive personal information.

2. Online organizations should take more steps to get my consent before they use my personal information for certain purposes (e.g., sending targeted email advertising).
3. Online organizations should take more steps to get my consent before they share personal information with other parties.

4. Online organizations should have better procedures to allow us to prevent them from collecting certain sensitive personal information.

5. Online organizations should have better procedures to allow us to prevent them from using personal information for certain purposes (e.g., sending targeted email advertising).

Access:

1. Online organizations should have better procedures to allow us to review at least some of the personal information about us that is stored in their databases.

2. Online organizations should have better procedures to allow us to correct at least some of the inaccurate personal information about us that is stored in their databases.

3. Online organizations should have better procedures to allow us to delete at least some of the personal information about us that is stored in their databases.

4. Online organizations should have better procedures to allow us to contest the accuracy of all personal information about us that is stored in their databases.

5. Online organizations should have better procedures to allow us to verify the accuracy of my personal information that is shared with other parties.

Appendix 4 (continued)

Security:

1. Online organizations should devote more time and effort to preventing unauthorized access to personal information.

2. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.

3. Online organizations should take more steps to make sure that unauthorized people cannot access personal information in their computers.

4. Online organizations should take more steps to ensure the secure transmission of my personal information.

Integrity:

1. All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.

2. Online organizations should take more steps to make sure that the personal information in their files is accurate.

3. Online organizations should have better procedures to correct errors in personal information.

4. Online organizations should devote more time and effort to verifying the accuracy of the personal information in their databases.

Appendix 5 Inter-Item Correlations by Scale

Notice

	N1	N2	N3	N4	N5
N1	1.0000				
N2	.6755	1.0000			
N3	.7197	.8068	1.0000		
N4	.7063	.7520	.6941	1.0000	
N5	.7607	.6944	.7586	.7597	1.0000

Choice

	C1	C2	C3	C4	C5
C1	1.0000				
C2	.7522	1.0000			
C3	.7508	.8580	1.0000		
C4	.7465	.8151	.7474	1.0000	
C5	.7625	.8432	.8680	.8131	1.0000

Access

	A1	A2	A3	A4	A5
A1	1.0000				
A2	.8386	1.0000			
A3	.7640	.7276	1.0000		
A4	.7787	.8650	.7646	1.0000	
A5	.7690	.8306	.7762	.9067	1.0000

Security

	S1	S2	S3	S4
S1	1.0000			
S2	.7407	1.0000		
S3	.8772	.7540	1.0000	
S4	.8340	.7849	.8539	1.0000

Integrity

	S5	S6	S7	S8
S5	1.0000			
S6	.7840	1.0000		
S7	.6993	.7956	1.0000	
S8	.7333	.8635	.7653	1.0000

Appendix 6 Mean and Standard Deviation by item

	N	Mean	Std. Deviation
Notice item 1	376	6.21	1.244
Notice item 2	376	6.29	1.266
Notice item 3	376	6.45	1.172
Notice item 4	376	6.16	1.352
Notice item 5	376	6.36	1.225
Choice item 1	376	6.24	1.292
Choice item 2	376	6.48	1.105
Choice item 3	376	6.54	1.133
Choice item 4	376	6.38	1.178
Choice item 5	376	6.46	1.154
Access item 1	376	6.22	1.241
Access item 2	376	6.16	1.242
Access item 3	376	6.30	1.261
Access item 4	376	6.26	1.210
Access item 5	376	6.30	1.179
security item 1	376	6.46	1.133
security item 2	376	6.39	1.117
security item 3	376	6.52	1.081
security item 4	376	6.48	1.076
security item 5	376	5.85	1.460
security item 6	376	6.04	1.336
security item 7	376	6.08	1.299
security item 8	376	5.96	1.412