PRIVACY CONCERNS AND PERSONALITY TRAITS INFLUENCING ONLINE BEHAVIOR: A STRUCTURAL MODEL

Brian C. Grams, B.A., M.B.A.

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

May 2005

APPROVED:

Linda Schamber, Major Professor
Randall E. Schumacker, Committee Member
Lawrence R. Wheeless, Committee Member
Brian O'Connor, Coordinator of the Information Science Doctoral Program
Samantha K. Hastings, Interim Dean of the School of Library and Information Sciences
Sandra L. Terrell, Dean of the Robert B. Toulouse School of Graduate Studies

Grams, Brian C., *Privacy concerns and personality traits influencing online behavior: A structural model*. Doctor of Philosophy (Information Science), May 2005, 258 pp., 16 tables, 11 figures, references, 71 titles.

The concept of privacy has proven difficult to analyze because of its subjective nature and susceptibility to psychological and contextual influences. This study challenges the concept of privacy as a valid construct for addressing individuals' concerns regarding online disclosure of personal information, based on the premise that underlying behavioral traits offer a more reliable and temporally stable measure of privacy-oriented behavior than do snapshots of environmentally induced emotional states typically measured by opinion polls.

This study investigated the relationship of personality characteristics associated with individuals' general privacy-related behavior to their online privacy behaviors and concerns. Two latent constructs, Functional Privacy Orientation and Online Privacy Orientation, were formulated. Functional Privacy Orientation is defined as a general measure of individuals' perception of control over their privacy. It was measured using the factors General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity as indicator variables. Online Privacy Orientation is defined as a measure of individuals' perception of control over their privacy in an online environment. It was measured using the factors Willingness to Disclose Online, Level of Privacy Concern, Information Management Privacy Concerns, and Reported Online Disclosure as indicator variables.

A survey questionnaire that included two new instruments to measure online disclosure and a willingness to disclose online was used to collect data from a sample of 274 adults. Indicator variables for each of the latent constructs, Functional Privacy Orientation and Online Privacy Orientation, were evaluated using corrected item-total correlations, factor analysis, and coefficient alpha. The measurement models and relationship between Functional Privacy Orientation and Online Privacy Orientation were assessed using exploratory factor analysis and structural equation modeling respectively. The structural model supported the hypothesis that Functional Privacy Orientation significantly influences Online Privacy Orientation.

Theoretical, methodological, and practical implications and suggestions for analysis of privacy concerns and behavior are presented.

ACKNOWLEDGMENTS

I want to thank my dissertation advisor Dr. Linda Schamber for the years of counseling and support she has provided. I always appreciated her openness and honest feedback during my doctoral education, and the guidance she provided that culminated in this research effort. She was a crucial force in my success. I also want to thank my committee members, Dr. Randall E. Schumacker and Dr. Lawrence R. Wheeless, for the guidance they provided in helping me complete this project. Their guidance, advice, and contributions in the fields of communication and measurement theory helped assure the success of this project.

I want to thank my wife, Janice, who was willing to tolerate my distraction for so many years. I also thank her for her understanding of my withdrawal from humanity for extended periods while I attempted to finish this project.

I also wish to thank Dr. Alan Scheibmeir of Grayson County College and Mr. Alvis Dunlap of the Denison Independent School District, their faculty, staff, and the students of Grayson County College for supporting my efforts.

Without the help of these people, and so many others, this effort would not have been possible.

TABLE OF CONTENTS

APPENDIX

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION TO THE STUDY

Introduction

In a context of uncertainty surrounding the nature of privacy, this study attempts to clarify underlying attitudes that contribute to the nature of individuals' behavior related to privacy. This chapter presents the background and reasoning that resulted in a study designed to explore influencing factors and personality characteristics precipitating privacy-oriented behavior. This endeavor comes at a time when accelerating rates of technological advancement, particularly communication-related technologies, continue to augment the collection and aggregation of personal information. This study is designed to enlighten a temporally stable underlying mechanism that contributes to individuals' privacy behavior in terms of personality characteristics, behavior, and concerns associated with the management of personally identifiable information fueling individuals' privacy-related concerns.

Privacy: Missing the Point

In Western culture, privacy has been debated in philosophical, legal, sociological, and too often in emotional terms. Philosophers, academics, and individuals find both physical- and information-based notions of privacy difficult to define. Contemporary experts on privacy have stated that privacy is essentially indefinable because of its contextual and personally subjective nature. Nevertheless, the majority of individuals

can without hesitation state their privacy has been violated. Coincidental to individuals' increasing concerns surrounding this vague concept of privacy, the use of technology to collect, analyze, aggregate, and market personally identifiable information continues to escalate. Individuals' privacy concerns and the growth of technologies that threaten the individual's concept of privacy are consistently targets for those who believe that the right of privacy is under attack and in jeopardy of being lost.

Individuals' inability to consistently explain why they think their privacy has been violated calls into question privacy as a useful construct for exploring individuals' concerns with respect to the collection and use of their personal information, and the oft-perceived violation of their privacy. A reasonable question that might be asked is whether the term privacy is being used as an overarching term for a number of conceptually related concerns, or simply a pretense in discussing individuals' concerns about actual physical access to them or their personal information. In either case, privacy is an ambiguous concept that, when addressed in terms of privacy concerns, appears tautological and may be counterproductive to providing solutions that benefit involved parties.

Realistically, the legal and regulatory environment associated with both physical and informational privacy plays an influential role in shaping attitudes about privacy. Legislation, regulation, and industry standards have been developed and implemented to protect many facets of personal information such as medical and financial information, information related to children, and physical aspects of privacy such as search and seizure. It is not the focus of this study to provide a detailed exploration of the legal and regulatory environments dealing with privacy in terms of physical access

or specialized information environments. Material related to these situations is explored because of its potential influence on the formation of attitudes related to privacy. This study is instead concerned with the underlying foundations of privacy-related behavior. It attempts to uncover privacy concerns associated with personal information that falls outside the venue of currently regulated or standard information management practices.

Problem Statement

Individuals, government, business, and advocacy groups constantly debate privacy and the proper management of personally identifiable information. Concurrently, individuals continue to express a high level of concern about privacy and the management of their personal information. People indicate privacy concerns are a barrier to adoption of new technologies. Yet people use new technologies, technologies that allegedly contribute to their anxieties about privacy, in a fashion that appears antithetical to their expressed concerns. This characterization, along with a continually expanding array of online technologies used by growing segments of the population, makes it apparent that people are not turning off their computers, PDAs, or cell phones and walking away from them in droves because of privacy concerns. Individuals may be using the language of privacy out of context due partly to the difficulty in defining the concept.

A tension exists between this broad acceptance of new technologies and its ever expanding and invasive uses. The nature and degree of impact that the privacy concerns of individuals have on technology acceptance and utilization, if any, are fodder for debate. The debate is fueled by the difficulty associated with empirically quantifying specific relationships between alleged privacy concerns, the nature of the individual

expressing those privacy concerns, and any resulting impact on actual technology-related behavior. A failure to reconcile and develop an understanding of these issues constantly presents stumbling blocks in efforts to effectively address them and provide beneficial approaches for all parties involved.

Purpose

This study was designed to provide perspectives on individuals' attitudes and concepts with respect to privacy and privacy-related behavior. The insight into the structure of privacy-related behavior was based on empirical evaluations of theoretically related substantive constructs commonly associated with privacy. In attempting to reconcile differences between privacy concerns and online behavior, this study will explore relationships involving an individual's personality characteristics or behavioral proclivities related to privacy. A number of constructs substantively associated with privacy behavior or attitudes were postulated as a new construct referred to as Functional Privacy Orientation. Functional Privacy Orientation was assessed using instruments designed to evaluate a number of theoretically related constructs. These instruments were designed to assess the latent factors of General Disclosiveness (Wheeless, 1978); defined in this study as a general willingness to share personal information through a message to another; Locus of Control incorporating Levenson's (1981) three dimensional interpretation; Generalized Trust (Wheeless & Grotz, 1977); and Risk Orientation and Risk Propensity (Rhormann, 2002).

The construct of Functional Privacy Orientation will be evaluated with respect to Online Privacy Orientation, conceptualized as an individual's general inclination to disclose personal information in an online environment. Online Privacy Orientation will

be evaluated using an indicator of the level of an individual's privacy concerns developed by Westin (Harris Interactive, 2002). In addition to Westin's measure, an approach developed by Smith, Milberg, and Burke (1996) will be incorporated that examines privacy concerns in terms of individuals' concerns about organizational management of personal information. Reported Online Disclosure and Willingness to Disclose Online, two new instruments developed for the study, are designed to augment the measurement of the latent construct of Online Privacy Orientation. The results of this study seek to improve the understanding of an individual's underlying privacy attitudes and the influence of those attitudes on Online Privacy Orientation. This goal is realized through a quantitative assessment of the relationship between Functional Privacy Orientation and Online Privacy Orientation. This study contributes to a better understanding of privacy than that garnered through the use of opinion polls and reactionary market behavior. This constitutes a different approach to understanding the relationship between online behavior and privacy-oriented behavior. The primary difference is that of an empirical evaluation of individual attitudes and behavior related to the contributing factors influencing privacy-related behavior. The concept of privacy has been, and continues to be, a focus for debate as a result of the impact of pervasive communication technologies and their influence on the management and use of personally identifiable information. The study was designed to show that use of the concept of privacy obscures any reasonable path leading to an amelioration of privacy concerns, and potentially enhancing beneficial information exchanges.

The findings of this study supplement and complement previous research that investigated relationships between individuals' perceptions or concerns related to

privacy and their behavior related to privacy. The majority of prior research was in direct marketing and telemarketing environments. Privacy concerns associated with direct marketing and telemarketing, in conjunction with the growing use of data processing systems, provided a catalyst for establishing the current general attitude of individuals toward privacy. These attitudes are fueled by the collection and use of personal information, and the emergence of a burgeoning information trade associated with the aggregation and utilization of that information.

The focus on privacy has proven to be a pivotal concern to organizations that utilize individuals' personal information, and a growing concern to individuals who provide that information. A number of studies and surveys have focused on rising privacy concerns. The majority of the studies have attempted to avoid the unpredictable and subjective nature of the privacy construct or otherwise failed to evaluate the underlying attitudes and perspectives that may contribute to the concerns individuals express about what they perceive to be the nature of privacy. This study did not attempt to reduce privacy concerns to any fundamental form or imply that they consist of a particular fixed group of underlying constructs. It is instead intended to contribute to an understanding of associated attitudes that may influence those concerns. This study demonstrates a relationship between a fundamental privacy orientation, referred to as Functional Privacy Orientation, and expressed concerns and behavior in online environments, referred to as Online Privacy Orientation. This relationship enhances an understanding of why, even though individuals articulate concerns about privacy, they exhibit behavior inconsistent with privacy concerns. The design of this study attempts to provide a conceptual framework that will reinforce prior efforts and assist in directing

future efforts that seek to reduce individuals' privacy concerns and enhance their online experience. This amelioration of concerns is intended to influence and provide a working understanding that will assist in establishing the basis of efforts in organizations seeking to attract and retain online relationships, or that seek to restore confidence in organizational management of personal information sought by the individuals they serve.

The concept of privacy is generally used to address an individual's concern regarding control of physical access, and access to or use of personally identifiable information (Phelps, Nowak, & Ferrell, 2000). Significant in the understanding of the concept of privacy are the four dimensions with respect to legal tort as described by Prosser (1960):

> (1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> (2) Public disclosure of embarrassing private facts about the plaintiff.
>
> (3) Publicity which places the plaintiff in a false light in the public eye.
>
> (4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. (p. 389)

The dimension of privacy described by Prosser as intrusion initially encompassed intrusive physical aspects of privacy, but now encompasses additional encroachments including electronic intrusions, exemplified by law-enforcement activities such as covert surveillance. The four dimensions are important because they define, in most circumstances, the total of protection available to individuals to safeguard or control access to themselves or their personal information outside the context of constitutionally-based protections. Common to all the dimensions is the informational

aspect of privacy, irrespective of tort-related dimensional differentiation. While the history surrounding many privacy issues is presented to help lay the foundations for this study, the focus of this study is on privacy related to personal information that is not subject to protections under legal tort and not regulated or constitutionally protected.

Personally identifiable information is defined in the context of this study as information associated with a specific individual. There is an issue that needs clarification at this point in the discussion. Personally identifiable information does not necessarily imply that the information associated with an individual was identifiable or associated with an individual at the time it was supplied. Seemingly anonymous information provided by an individual to any other individual or organization is often associated with the individual without the provider of the information supplying any identification. This association between anonymous information and information provided with identification can be made through the use of profiling, a process or procedure incorporating data mining or data aggregation techniques. For the sake of clarity and ease of reading, personally identifiable information is referred to here as personal information, private information, or simply as information in the framework of this study.

Research Questions

The concept of privacy appears, from the perspective of the individual, to buttress the desire not to reveal personal information. But individuals often choose to share personal information that is not common knowledge or knowledge they would willingly share with just anyone. To reveal information about oneself, or communicate a message about oneself to another is a construct often referred to in the literature as

self-disclosure (Jourard, 1971; Wheeless & Grotz, 1976). It has also been proposed and investigated as an individual trait in that individuals may show a more general tendency to self-disclose. The more generalized tendency to self-disclose is a factor referred to as General Disclosiveness (Wheeless, 1978). The tension between the desire for privacy and the choice to reveal oneself is referred to by Petronio (2002) as boundary management in her theory of communication privacy management or CPM. Disclosure, and the concept of boundary management related to disclosure, has become more significant in the everyday life of the individual. The significance is particularly evident with respect to the pervasive collection and aggregation of information in the current technology environment.

This tension between desire, decision, or choice involving privacy and disclosiveness has led to a number of questions that were addressed in this study. The research questions relate to behavioral characteristics associated with disclosure and privacy concerns. This study explores the direction, strength, and the interrelationships of attitudes with respect to a number of factors or constructs. The factor Functional Privacy Orientation, as conceptualized, was investigated using a number of reflective indicators that theoretically impact, or are related to the individual's decision to disclose. The factors postulated as reflective indicators of Functional Privacy Orientation are General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity. The study also investigates the levels and dimensions of privacy concerns individuals possess with respect to management of their information, online disclosure, and the individual's perceived willingness to disclose online. The relationship of these

reflective indicators are conceptualized as the factor referred to as Online Privacy Orientation. This approach is designed to address the following research questions:

1. What is the relationship of Functional Privacy Orientation to the multidimensional constructs General Disclosiveness, Locus of Control, and Risk Orientation and to the unidimensional constructs Generalized Trust and Risk Propensity?
2. What is the relationship between Willingness to Disclose Online, Level of Privacy Concern, the four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection), and Reported Online Disclosure?
3. Does Functional Privacy Orientation predict Online Privacy Orientation?

These questions are addressed with the objective of adding to the body of research that speaks to the conflict between individuals' concerns about privacy and their underlying behavior associated with privacy. Unlike prior studies, this objective was accomplished through an empirical evaluation of social psychological and information-related behavioral characteristics. Unlike the majority of prior investigations, this study incorporated an analysis based on theory that deals with underlying personality characteristics related to the concept of disclosure, a fundamental construct related to privacy.

Hypotheses

The research questions result in a study designed to test four hypotheses that explore the relationships between individuals' Functional Privacy Orientation, its supporting constructs, and Online Privacy Orientation and the relationships of its supporting constructs.

The literature dealing with privacy and disclosure persistently brings up the concepts of control, trust and risk. Many business efforts to address individuals' concerns about privacy have been approached by the business community in the past through organizations such as the Better Business Bureau® (Better Business Bureau, Arlington, VA, www.bbb.org), and online in the form of privacy-oriented organizations such as TRUSTe® (TRUSTe, San Francisco, CA, www.truste.org). These efforts rarely deal directly with individuals' desire to have some semblance of control over their personal information. However, the matter of control consistently emerges in discussions about individual privacy concerns. Difficulties arise in assessing whether business efforts to address privacy issues are actually addressing the correct issue. The following hypotheses endeavor to address these difficulties.

H_1: Locus of Control/internal is influenced significantly more by Functional Privacy Orientation than Generalized Trust.

H_2: Locus of Control/internal is influenced significantly more than either dimension of Risk Orientation by Functional Privacy Orientation.

Levenson's (1981) instrument evaluates the construct of Locus of Control on three dimensions; chance, powerful others, and internal. Individuals who believe they possess a higher level of control over life events should not portray as high a level of dependency on general trust, or perceive as great a risk from their surroundings as individuals who believe powerful others or chance significantly influence their situations.

H_3: The four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection) will load inversely to Online Privacy Orientation with respect to Reported Online Disclosure.

While this proposition would seem intuitively apparent, evaluating privacy concerns with respect to disclosure will provide statistical insight into individuals' expressions of concern garnered from opinion polls. H_3 supports currently advocated viewpoints that an individual's hesitation to share personally identifiable information is a function of privacy concerns. These viewpoints have been evidenced in both privately funded studies and anecdotal evidence, pointing to the fact that the online exchange of personal information between individuals and organizations has been inhibited, resulting in impeded services and lost business revenue (Cyber Dialogue, 2001; Louis Harris & Associates, 1999). The study was designed to demonstrate empirically the factors Willingness to Disclose Online and Reported Online Disclosure have an inverse relationship to privacy concerns; that is, the higher the level of individuals' concerns about privacy, the less likely they are to share personal information. This exploration will operationalize a theoretical approach that should provide support for or conversely challenge findings that have been reported in prior opinion surveys.

Research Question 3 inquires into the nature of the relationship between individuals' Functional Privacy Orientation and Online Privacy Orientation. As stated earlier, individuals do not appear to be abandoning communications technology as a result of professed privacy concerns. That is not to say that their concerns do not impact their use of the technology. H_4 attempts to address the question of the potential impact to Online Privacy Orientation of individuals' perceptions of the increasingly pervasive use of communications technologies to gather personal information.

H_4: Online Privacy Orientation is significantly influenced by Functional Privacy Orientation.

Privacy concerns have been associated with a reduced level of online disclosure. In 1996 Smith et al. developed, tested, and validated a survey instrument delineating individuals' focus on four primary areas, or dimensions, of privacy concerns in online environments and the level of concern associated with each. The four primary dimensions are (1) concerns about errors related to collection and maintenance of personal information, (2) improper access to personal information, (3) unauthorized secondary use of personal information, and (4) collection of personal information.

Westin (Harris Interactive, 2002) developed a measure of a more general level of an individual's privacy concern with respect to online behavior. Westin segregated the respondents into three groups or levels of privacy concern based on answers to three statements. (1) Privacy fundamentalists are very concerned about the collection and use of their personal information. They are characterized as being protective of their information and reluctant to disclose. (2) Privacy pragmatists evaluate information requests and release information based on their assessment of risk and reward based on each unique situation. The level of concern is moderated by the situation and actual release of information may be interpreted as a function of the level of concern. (3) Privacy unconcerned individuals are prone to release information to anyone for any reason. Westin's characterizations parallel the level of concerns depicted in the results obtained by Smith et al., providing a less refined but more generalized measure of privacy concern. It is anticipated that an increased level of concern related to organizational management of personal information, and an increased level of concern characterized by Westin's instrument will show a significant inverse impact with respect to either a willingness to disclose or actual disclosure in online environments. The

model developed for this study will attempt to discern a differential between modifiers to Online Privacy Orientation and relate this to individuals' Functional Privacy Orientation.

Significance

A number of issues surrounding the concept of privacy and personal information were addressed in this study. The concept of privacy in individuals' concerns regarding use of their personal information and impacting Online Privacy Orientation was empirically tested. The findings of this study are intended to demonstrate a segregation of concerns related specifically to Online Privacy Orientation that may be dealt with individually, providing opportunities or steps that can be taken by organizations and individuals, to reduce the level of anxiety individuals experience when faced with the opportunity to share personal information in an online environment. The findings of this study will provide an empirical foundation by demonstrating that the willingness to share personal information online is less a function of behavioral characteristics of the individual with respect to privacy, and more a function of concerns related to the management of their personal information.

Potentially the most significant contribution will be a departure from the historical opinion poll to evaluate privacy concerns with respect to the sharing of personal information in online environments, to a broader empirical investigation of how individual perspectives on privacy may be more effectively evaluated.

The findings of this study will also contribute to a growing body of literature that has the potential to promote more effective policy formulation and regulation for improved management of unregulated personal information. Current approaches to regulation, whether self- or government-imposed, appear unable to address the growing

concerns of the public with respect to the increasing amount of unregulated information collected on individuals. Governmental bodies, organizations, businesses, and individuals all have the opportunity to benefit from an enhanced flow of information based on improved information management practices. This study is intended to demonstrate that improved information management practices, based on an analysis of findings, could be accomplished most effectively with minimal government intervention and offer guidance on the most effective methods of government oversight necessary to maintain compliance with guidelines for improved information management practices. The success of organizations that seek to self-regulate personal information management practices must address a broader range of influencing factors to prevent an attitude backlash such as that described by Sheehan (2002). As a result of this effort, organizations that collect and utilize personal information will have a clearer understanding of the issues and concerns that need to be addressed, putting the amorphous concept of privacy aside and dealing with more concrete issues.

The results of the study will also provide further empirical support, and contribute to a better relational understanding of self-disclosure as a personality characteristic or construct in studies relevant to communication, psychology and social psychology.

Methodology

Data were collected using a survey instrument developed specifically for this study. This instrument, referred to as the Privacy Disposition Inventory, consists of both previously used and tested instruments and newly developed instruments. The PDI consists of three primary sections made up of a collection of nine instruments. Seven of the instruments have been used to explore their respective constructs and were

subsequently evaluated with respect to reliability and validity in prior research. Two instruments designed to assess online disclosure and willingness to disclose online were developed specifically for this study. A final section collected demographic data.

The first portion of the PDI is made up of five instruments that deal with constructs related to the postulated latent construct of Functional Privacy Orientation. The constructs evaluated in the context of Functional Privacy Orientation are General Disclosiveness, Locus of Control, Generalized Trust, and Risk Orientation and Risk Propensity. All of the instruments other than Generalized Trust and Risk Propensity measure multiple dimensions on the underlying latent construct. The second section is made up of four instruments intended to evaluate the postulated latent construct Online Privacy Orientation. Two of the instruments for evaluating the dimensions and level of an individual's privacy concern were developed and used in prior research addressing those issues. A third instrument is a self-report of the participant's last online experience, and the fourth is a self-report of willingness to disclose online. These last two instruments have not been used previously. I was not able to locate any previously developed instruments designed to evaluate these two areas of interest. Validity and reliability were addressed in the context of the analyses.

The primary group of participants came from a semi-rural community college. The sampling may be justifiably characterized as a convenience sample but offered a high potential in sample variability. The intent in choosing this source of participants is the diversity of the student body, faculty, and staff. The focus of community college charters is on technical education and certification, continuing education, workforce training, and corporate training. This focus is in addition to the standard freshman and

sophomore level academic courses common to colleges and universities. This type of educational environment may potentially provide a more diverse student population with respect to age, experience, and education than a typical college or university campus.

A number of other sources of survey participants were also utilized. These included the faculty and staff of a Texas middle school, the faculty and staff of a private day school, and small business owners serviced by a local distribution company. These additional opportunities were expected to add approximately one hundred observations. The additional participants were intended to contribute to a more diverse sample, potentially enhancing generalizability.

Reliability of previously developed instruments was addressed using Cronbach's α. Corrected item-total correlations and exploratory factor analysis were incorporated to evaluate previously unpublished results from the risk instruments and the two new instruments dealing with online disclosure and willingness to disclose online. A structural model consisting of the two new latent constructs was evaluated using structural equation modeling. Assessment of the measurement models and structural model included chi-square and various other fit criteria. The full structural model with the measurement models are presented in the methodology in chapter 3. This approach to analysis, exploratory factor analysis, and structural equation modeling, were selected for a number of reasons including explicit estimates of measurement error and the ability to simultaneously assess both latent and observed variables. These and other advantages are discussed in greater detail in the chapter 3.

Summary

This chapter has presented the reasoning for, the approach to, the background on, and the significance of the proposed research effort. A series of research questions and related hypotheses were posed that constitute the objectives of this research in terms of what was addressed, that is an improved understanding of underlying factors that influence online behavior. An overview of the proposed methodology, and analytical methods intended to address the research questions and hypotheses were also briefly presented with a short explanation of the benefits of the proposed approach. The remaining chapters will provide an in-depth presentation of theoretical foundations supporting the design of the study, the methodology incorporated in executing the study, the findings, and a discussion of the results.

CHAPTER 2

BACKGROUND

Introduction

The concept of privacy is shaped by a lattice of interwoven realties and perceptions that defy a narrow or focused approach to its understanding. Social, psychological, environmental, legal, and moral influences are but a few of the contributing factors that present a quagmire of understanding and behavior constituting the normative view of privacy. Varied approaches have been taken by any number of philosophers, researchers, lawmakers, businesses, and individuals in attempts to comprehend the basic nature of this concept. All these individuals or groups have made material contributions, and all have been influenced by factors that impact perceptions related to privacy. Stated more simplistically, there is not a direct approach to be had to explore the concept of privacy.

This chapter reviews substantial influences related to privacy that are the products of thought in philosophy, research, and normative reality that impact the formulation of perspectives on privacy, the nature of the responses observed, and the resulting privacy environment. It will also assist the reader in understanding the foundations of the concept of informational privacy. The literature is used to establish the links between the constructs being used to measure privacy-related behaviors,

resulting in a framework supporting the conceptualization of a model that forms the base for this study.

The Subjective Nature of Privacy

Establishing a meaningful framework for the concept of privacy has proven elusive. The concept of privacy has been approached in terms of social interaction, a social control mechanism designed to promote social freedom (Schoeman, 1992) and attain social goals, constitutionally as an individual right or entitlement (Schoeman, 1984), or a fundamental "…right to be let alone…" (Warren and Brandeis, 1890, p. 193). Westin, in his seminal work, *Privacy and Freedom* (1967), proposes that the individual perceives privacy as control over the flow of information about oneself and ". . . the voluntary and temporary withdrawal of a person from the general society through physical or psychological means …" (pg. 7). The perception of privacy appears to derive from individuals' control over personal information and control of access to their persons (Solove, 2002).

Schoeman (1992) sees privacy as a social mechanism that provides independence for an individual to act without fear of reprisal or social repression. Fear of reprisal, individual autonomy, freedom of speech, and protection from governmental control and intrusion have all been cited as fundamental rights or liberties granted by virtue of the right to privacy. Privacy also possesses less positive characteristics. Schoeman (1984) believes that some view privacy as a veil, behind which immorality and social deception are allowed to flourish.

These perspectives give credence to privacy as a concept, but none effectively defines privacy in terms that may be applied both universally and uniformly. This raises

a specter of ineffability that has been a hallmark of the privacy issue. By virtue of its fluid definition, privacy presents itself as a pragmatic and important social issue, functionally necessary in a social context, but virtually impossible, without contention, to scrutinize in terms of a practical concept leading to the development of practical means to address privacy issues.

It is important to clarify an issue that commonly confounds discussions surrounding privacy. The issue is the requirement of a differentiation between the concepts of privacy and security. In the context of this study, and in a general context, information security deals with the physical integrity or protection of information. The concept and use of the term referred to as privacy deals with the collection, use, or dissemination of the information, not with its physical security. This is not to say information security and privacy are conceptually isolated from each other with regard to concerns about personal information. The distinction is drawn because of the tangible nature of information security and the intangible nature of privacy. Privacy and related concerns, the focus of this study, persistently emerge as fuel for the constant debates regarding personal information. Information security is addressed from a predominantly functional or physical perspective.

Privacy, as evidenced in the earlier discussion, is multifaceted and complex. The inability to effectively characterize privacy leaves individuals relatively unencumbered to define and invoke their perceived privacy rights, rights that appear to originate simply through their own claims to privacy. These claims may be substantiated in cultural behavior, related legal rights, or through the beliefs or understandings developed by the individual.

There have been a number of approaches in attempting to define and investigate the concept as well as a history related to attempts at addressing it, that provide the opportunity for logical partitions in addressing privacy. In order to better understand some of the issues related to addressing privacy I will break down the concept into general classes that surface in the literature. The partitions I propose in order to simplify and focus the discussion deal with privacy in the context of government, business, and individual characteristics. No definitive boundary exists between these categories, and all exhibit commonalities, but establishing some type of differentiation will aid in focusing the topic of this study. Each of these categories is significant in the context of this study. In one respect they aid in isolating various aspects or views of privacy and the related concerns. In another respect they facilitate focus on the less well understood and hence the more arguable concerns surrounding privacy.

Origins of the Current Privacy Debate

Privacy plays an important social role. Its influence is seen not only in modern normative social behaviors but also in primitive cultures (Westin, 1967). Concepts of privacy have changed over the course of history and in many instances have developed as a result of social and technological influences (Schoeman, 1992). It appears that current conceptions of privacy were developed as a result of technological innovation, notably by improvement in communications technologies. In the seminal article by Warren and Brandeis in 1890, and later in Justice Brandeis' dissent in *Olmstead v. United States* (1928) the concept of privacy was brought into public focus. Warren and Brandeis accomplished this using a characterization by Judge Thomas Cooley of the Michigan Supreme Court, who addressed the concept of privacy with the phrase "the

right to be let alone" (DeCew, 1997, p. 14). In 1880, the year Cooley penned this phrase, privacy had yet to become a significantly publicized concern to the individual. At the time Warren and Brandeis released their article in the *Harvard Law Review*, the primary concerns related to privacy focused on physical encroachment and invasion of one's privacy by the press. Privacy as a public issue or concern has continued to develop and significantly changed with the ongoing rapid development of communication technologies.

In the last several decades computer technologies in general, and most recently the Internet and the World Wide Web, have provided a rich setting for the rapid and open exchange of information. Individuals, along with all types of businesses, organizations, and governmental agencies have recognized the potential benefits of this effortless and rapid flow of information. Unfortunately, some opportunistic individuals and organizations have failed to recognize risks that this free flow of information could potentially present in terms of individuals' privacy concerns and safety.

Individuals have recognized and benefited from the wealth of information available at their fingertips. Literature has documented well the benefits of this wealth of easily accessible information to both organizations and the individuals the organizations serve. The problematic issues associated with this new technology have not been so clearly addressed. It is important to review some of these issues to better understand why privacy has become a focus of individual concern and so vigorously debated.

Personal Information and Practical Obscurity

Prior to extensive online access to public records, most personal information contained in public records was protected by practical obscurity (EPIC, 2003). Practical

obscurity refers to the fact that even though personal information is publicly available as a component of public records, the actual physical retrieval of the information is hindered by distance, convenience and access boundaries. As an example, before the advent of easily accessible electronic records, public records were readily available regarding John Doe's bankruptcy in another state. Doe's privacy was maintained by the fact that he did not normally have to worry about his new neighbors in his new state of residence discovering this information without a directed and significant effort on their part. Electronic access to public records has removed or reduced the barriers of distance, time, and cost associated with finding information about John Doe. Anyone with World Wide Web access can now search public records over the Internet or pay a small fee to an online company to perform the search, revealing the most intimate and minute details of an individual's background or history with minimal effort.

Unfortunately, in this and similar contexts, unfettered information flow has potential negative consequences (Cyber Dialogue, 2001; Louis Harris & Associates, 1999). Many individuals prefer that their neighbors, or anyone else for that matter, not have easy access to intimate details of their personal life, even if these are a matter of public record. Individuals have recognized that personal information, now quick and easy to access, is potentially harmful or risky in social, financial, health benefit, employment, personal safety, and numerous other contexts. This potential for harm in the form of misrepresentation or inaccuracy of facts, or simply unfettered access, creates anxiety and modifies behavior or attitudes, resulting in individuals creating barriers to or resisting the free flow of information. The process of dealing with these

issues and anxieties leads to the loss of dollars and opportunities for all involved parties.

Opinion surveys have repeatedly established the fact that individual consumers are concerned about their privacy (Cranor, Reagle & Ackerman, 1998; Harris Interactive, 2002). Legislative bodies and privacy advocates invoke this concern as a basis for developing and proposing guidelines for the management of personal information. Business organizations contend that access to increased levels of detail in customers' or a clients' personal information provide substantial benefits by forming a foundation for a more efficient and effective business model. They assert that the information they gather has the potential to benefit all involved parties. Conflict and disagreement in privacy-related matters stem from individuals' privacy concerns and organizations' information-related goals.

Technology's Impact on Privacy

The role of technology and its influence on privacy is well documented (Garfinkel, 2000; Miller, 1971; Westin, 1967). Beginning in the 1960s, computer technology was beginning to have a significant impact on the manner in which organizations carried out their missions or conducted their business. Database development, electronic mass storage, and information retrieval techniques began to provide easier access to larger amounts of information about virtually everything, including detailed information about organizations, their customers, members, or workforce, or any other venue where records are kept on individuals. Governmental agencies such as the Internal Revenue Service, the Social Security Administration, the Bureau of the Census, and government intelligence organizations were also able to benefit from the ease of access and

manipulation of information that computers provided. As the costs have fallen, the prevalence of technology has grown. As a result, the functionality or benefits of practical obscurity have become ineffective.

The true nature and basis for an individual’s concerns about privacy are sometimes questioned in light of the fact that numerous privacy-enhancing technologies are currently available but infrequently used. This apparent lack of concern is corroborated by the fact that there appears to be apathy or reluctance on the part of individuals to utilize these technologies to protect their privacy. Two major obstacles are lack of motivation and technical expertise. Failure to adopt privacy-enhancing technologies may simply be a case of technological naivety, not a lack of concern about privacy. Additionally, organizations may fail to adopt the technologies due to initial and ongoing costs, and individuals have the power to demand that the technologies be adopted.

Privacy and Organizations

There is a tension between entities that collect and use personal information and individuals who become the focal point of those entities' interests. Organizational entities have rights and responsibilities associated with personal information due in part to laws, regulations, and business practices. The level of individuals' awareness or perception of organizational perspectives significantly affects their expectations and behavior. This is particularly true with respect to their behavior in disclosing personal information hesitantly in one instance but willingly in another. A general description of organizational policies and practices, in both the public and private sector, is relevant to this discussion.

The Government: A Right to Demand Information

Government, at almost all levels, has the right to demand different types of information from citizens under its jurisdiction, often finding it critical to the successful execution of their obligations. For the individual citizen dealing with a government agency, providing requested information is generally not an option, but a legal requirement. This right of government to collect information does not necessarily stop with government demanding information from individuals but extends to many nongovernmental organizations as well.

A common example is that of Federal, state, and local government bodies requiring social security numbers from individuals to facilitate identification. As a consequence many individuals become accustomed to releasing this piece of personal information. If an individual is in a government office dealing with government officials and is asked to provide a social security number, there is little or no hesitation in providing it. Consequently, individuals become accustomed to providing their social security numbers for identification, and when requested by nongovernmental organizations for purposes of identification, it is generally provided. There is an interesting and well known caveat related to this situation; the social security number was never intended to be used as a means of individual identification. Even though this is true, individuals invariably encounter significant difficulties in conducting business if they refuse to provide it on request. Persistent demands, and the general acceptance of the practice by both individuals and organizations result in desensitization to such requests.

Furthermore, the requirement to provide personal information to governmental entities is on occasion enforced under penalty of law. The right of government to demand information from its citizens invokes certain responsibilities for the management and protection of personal information. As privacy continues to garner attention, federal and state governments have responded with legislation and regulation to protect various groups of individuals and types of information. Unfortunately, efforts to protect personal information in government jurisdictions have been inefficient and poorly organized.

In contrast to legislation protecting privacy, the government must contend with contradictory legislation under the Freedom of Information Act. Government agencies are required, under certain guidelines, to release information in public records to the public upon request. This apparent conflict in managing and releasing information creates confusion for individuals whose information is contained in the public record. It also creates confusion and difficulties for the governmental agencies responsible for protecting its citizens. So a conflict arises between obligation and perception related to both collection and dissemination of personal information. This arouses privacy concerns in two ways, the first being the concerns over the Orwellian specter of Big Brother, an all-seeing all-pervasive government with a legal right and obligation to collect personal information, and the countervailing demand and legal obligation of the same government to release the information that it has collected.

The Government and Individual Privacy Concerns

Since the privacy declaration of Warren and Brandeis (1890), privacy has come to be viewed as a right. The right to privacy is not specifically stated in the Constitution

as a right of all citizens, even though studies have shown that many believe it should be. The right to privacy is generally supported under the First, Third, Fourth, Fifth, and Fourteenth amendments (Cate, 1997; DeCew, 1997). In the 1965 Supreme Court case *Griswold v. Connecticut* the Justices also refered to the Ninth Amendment's language of unenumerated rights as establishing a penumbral right to privacy (Relyea, 2001). Under the pretext of unenumerated rights, the Constitution and Bill of Rights of the United States grants its citizens, as individuals, specific rights and protections that do not explicitly refer to a right to privacy but is interpreted from the language of the documents.

This constitutional framework has provided a foundation for the protection of an individual's privacy in a variety of contexts. Among these are protection against unreasonable search and seizure, freedom of speech, self-incrimination, and the protection of due process of law. What may not be patently obvious to individuals is the potential impact of nondescript information about them, information they generate about themselves in their everyday lives both online and offline. This impact is a consequence of the reality that even the most physical of dimensions, such as strolling down the street, are likely to become digital information stored in a governmental, organizational, or some individual's private database. Once something is digitized, such as an image of someone strolling down the street, it is available to share, sell, or ship anywhere in the world almost instantaneously. Technologies, such as picture phones, have allowed individuals to intrude on others' privacy, collecting, digitizing, and transmitting information on other individuals with even greater ease and rapidity.

Although laws supporting a right of privacy may be viewed as fractured and contextually specific, they have nonetheless afforded an expectation of protection of privacy rights on the part of the individual. This expectation affects individual's perceptions and behaviors with respect to privacy. The governmental response to privacy concerns recognizes some of the risks previously outlined. Unfortunately, much of the legislation has been purposely vague, relatively unenforceable, narrow in scope, and reactionary. It is briefly noted that the constitutionally supported right to privacy is separate from the tort protection described by Prosser (1960). Tort protections for privacy will be discussed in more detail later in the chapter.

A problem with individual perceptions with respect to privacy lies in the fact that the government is regulated to a much greater degree than non-governmental organizations regarding the release of information such as social security numbers. Quite often individuals become aware of the illegal or illegitimate uses of their social security numbers, such as in the case of identity theft, and subsequently become sensitized to the ramifications of the release of their information. Thus, on one hand individuals provide the information with little hesitation, while, on the other, they become more concerned regarding how it might subsequently be used. Further exacerbating the problem is the fact that following the release of personal information, particularly in an online environment, there is little if anything an individual can do to control how the information will be used.

A second influencing factor, other that the legal right or obligation to collect personal information, is the legal requirement for government to release information it collects. This required release has two facets. One facet is maintaining open public

records to allow the public to monitor governmental activity in an oversight capacity. This accountability helps to assure the public that elected officials and government organizations are performing their duties in a responsible manner. A second facet, the Freedom of Information Act serves as a legal mechanism that provides for the release of government information that is generally not part of open records. If governmental entities fail to provide requested information, an individual has the right to make a formal request for that information. The government is obligated, within certain guidelines, to comply with the request.

The required release of information diverges from the need to protect the citizenry from unwarranted releases of personal information. In its efforts to comply with information requests the government has recently, in the last decade or so, started placing information online so it may be accessed through the World Wide Web. Consequently, information such as criminal records, court proceedings, litigation, tax defaults, bankruptcies, the physical location of an individual, and a large body of additional information about individuals is now readily available. Records that were physically isolated and difficult to obtain are now available, either free or for a fee of a few dollars, with a simple online inquiry. Consequently, individuals have become sensitized to the release of their information that becomes a part of the public record. For someone who has an arrest record, or experienced financial difficulties, but has paid the debt society required to atone for these mistakes, the effort to return to society as a fully functional individual is hampered. As Blanchette and Johnson (2002) pointed out, the concept of social forgetfulness, which provides the individual a chance to start

over again, is being lost. Not only are individuals' present factual details readily available, a permanent digital record of their past is easily accessible to anyone.

Solove (2001) illustrates the human condition with respect to privacy and government held personal information and effectively puts the situation into perspective in his allegorical analysis of Kafka's book, *The Trial*. Solove analyzes the current metaphor of Big Brother with respect to invasion of privacy, and the currently prevalent conceptions this metaphor invokes with respect to the governmental collection of personal information. Solove holds that *The Trial* offers a much more effective metaphor for current privacy concerns by depicting the dehumanizing aspects of the current privacy environment. Solove contends it is not necessarily the image of Big Brother that raises privacy concerns for the individual, but the sense of loss of control and vulnerability as portrayed in *The Trial*. It is in this open yet regulated environment of privacy that individuals are required to function, forced to expose themselves to incalculable risks, and unable to resolve the onslaught of newly emerging and personally threatening assaults on their privacy. This situation does little to allay perceptions of risk and vulnerability and only enhances the sense of loss of control over personal information.

Constitutional protection often provides an illusion of privacy protection to the individual that does not effectively exist. Constitutionally the individual is primarily protected from only the most invasive privacy encroachments perpetrated by governmental organizations. It does not protect the individual's privacy from the person with the picture phone, or the business organization building information profiles based on information it acquired online, or from public records housed in county seats or other

government offices, financial information, phone bills, purchase histories, warranty registrations, or multitudes of other readily available sources. Constitutional privacy protection is probably more confusing or misleading than individuals realize.

There is another legal barrier protecting the information privacy of individuals. Outside of constitutional protection, legal recourse for protecting individuals' privacy is addressed in tort or civil law. The introduction to this proposal briefly addressed the dimensions of legal protection provided to an individual in tort or civil law. Prosser (1960) delineated these as:

> (1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> (2) Public disclosure of embarrassing private facts about the plaintiff.
>
> (3) Publicity which places the plaintiff in a false light in the public eye.
>
> (4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. (p. 389)

The difficulty with the nature of these dimensions of tort protection lies in the necessity that the plaintiff, generally an individual, must prove harm. The protection afforded is not designed to stop or preclude various types of behavior; it is intended to provide recourse for individuals who can prove that they have been damaged by someone, or some organization's actions involving access to or use of information about that individual. The burden of proof, and the essence of the protection, lies with the individual and not the information user. An individual should not believe that this protection of the law is preemptive.

A few remaining information privacy protections afforded individuals generally lie in three primary areas: international protections, regulatory protections, and self-

regulation. International protections are outside the scope of this study and are only mentioned for the sake of comprehensiveness. Other countries, in particular the European Union, have instituted stringent regulation of personal information. The resulting protection does not impact an individual's information privacy related to information held in the United States except for the case in which an American business organization is also operating overseas. These organizations have had to comply with information privacy standards instituted by members of the European Union in order to continue doing business in member countries. This point is made in order to exemplify the capabilities of American businesses in addressing privacy concerns if required. Even though many American companies are able to respond to the privacy requirements under safe harbor in the European Union it is considered too costly or cumbersome to institute these types of measures in the United States. The next section deals with the legislative and regulatory environment in which U.S. organizations are required to operate.

Legislative and Regulatory Responses to Privacy Issues

It is important to establish an understanding of the legislative and regulatory environment that surrounds the management of personal information collected and maintained by the government agencies, businesses, and other organizations. This discussion is relevant to the nature of this study because it demonstrates a level of protection that may still be misinterpreted and confusing to the individual.

Unlike protections provided by the United States Constitution, or legal recourse under tort law, regulations stipulate specific criteria under which certain types of information may be used. These regulatory requirements typically carry the force of law.

As such, in the case of regulation and law, the burden no longer lies with the individual to prove harm. The burden is shifted to the information consumers to prove that they are adhering to the guidelines laid out in law. The collection and management powers of government over private information, coupled with the roles and responsibilities of government agencies, result in the confusion and problems previously described.

Common threads of public concern exist in the area of privacy. Individuals perceive risks associated with other individuals or organizations collecting, possessing or being able to obtain details of their daily activities or personal history. Individuals also perceive risk associated with a loss or lack of control over information about them.

Governments and some business organizations have attempted to allay these fears by adopting a set of standard information practices. Some information practice guidelines were proposed by the Department of Health, Education and Welfare (now known as the Department of Health and Human Services) in 1974. These recommendations were developed as the result of a study attempting to address issues surrounding public information on individuals held by the government. These Fair Information Practices have been embraced by national and international organizations. The European Union demonstrated acceptance of the standards and developed a body of policy that uses them as a guideline for government regulation of the collection, use, and distribution of personal information.

The United States government has also adopted a number of policies and regulations related to online privacy. Personal financial information, information gathered from children, personal health information, and a number of other areas are covered by legislation and regulations intended to protect the personal information of a

number of specific groups of individuals or areas of information considered sensitive. Early privacy legislation included the Fair Credit Reporting Act, protecting consumers from inaccuracies in their credit files, and the Privacy Act of 1974, protecting federal employees from the disclosure of personal information. An individual's financial information is regulated under the Gramm-Leach-Bliley Act and children under the age of 13 are protected under the Children's Online Privacy Protection Act of 1998.

Outside the venue of currently regulated information the story is somewhat different. The government has resisted the appeals of privacy advocates, and taken into consideration the business communities objections to regulate the flow and exchange of most sources and types of personal information. This approach is counterproductive to efforts by members of the European Union adopting what is referred to as fair information practices, and has created significant friction regarding privacy and the management of personal information.

The Business Perspective on Privacy

Business sees significant potential in the ability to gather, store and analyze large amounts of data on individuals. Business believes this capability offers the opportunity to effectively target current and future customers who are likely to buy their products or services.

The primary objective for any business is enhancing the value of the company. One means of enhancing company value is through increased profits. Business recognizes the profit enhancement and savings potential in being able to effectively predict market trends and target market niches. Business can address this profit

potential with enhanced efficiencies and effectiveness made possible through information collected on individuals in the intended market.

Business also recognizes a need to protect customer information, if for no other reason than that of maintaining a competitive advantage. This does not preclude the sharing of data with other internal profit centers or external business partners.

Personally identifiable information is also viewed as a business asset that enhances company value. The depersonalization associated with viewing a customer's personal information as a company asset has recently come under public pressure. Examples abound that demonstrate the treatment of personal information as a company asset. Several scenarios can be cited which raise privacy concerns, such as the case of online retailers going through bankruptcy proceedings selling customer lists. This practice of attempting to classify customer information as a liquid asset was particularly prevalent in the last few years as a result of the collapse of the technology bubble that formed during the Internet/World Wide Web boom. Other business ventures proposed combining personal information from diverse sources, such as the DoubleClick® and Abacus® (DoubleClick Inc., New York, NY) data merger proposal, information brokers such as Equifax® (Equifax Credit Information Services Inc., Atlanta, GA) teaming with Lotus® (Lotus Development Corporation, Cambridge, MA) to sell large databases of personal information, or America Online® (American Online Inc., Dulles, VA) sharing phone numbers with outside marketing organizations. Each of these examples demonstrates the business perspective of information as an asset. These types of situations have not raised the individual's level of confidence in business management

of personal information but have instead created privacy concerns that are explored in the context of this study.

Business has the ability, inclination, and motive to share personal information. The multinational character of many corporations, in conjunction with enhanced data processing and telecommunications capabilities, along with emerging technologies such as the Internet and World Wide Web, has facilitated the sharing of personal information with international subsidiaries and other companies around the world.

Privacy in the Business Environment

Private sector organizations have been required to respond to privacy concerns on a number of fronts. The regulatory environment has created a need to respond to government mandates or face sanctions, censure, fines, or other punitive measures. Customers irritated by an organization's privacy practices have responded with protests and adverse activity resulting in loss of revenue, legal challenges, and loss or damage of the organization's reputation. A number of individual and consumer advocacy organizations have acted as watchdogs, monitoring and reporting on questionable activity regarding privacy in organizations. Business has also had to respond to privacy concerns in the international arena. This is due in large part to the European Union policies surrounding the use of personal information.

In almost every instance the business response has been the result of external pressure. The majority of business leaders (76%), as early as 1978, indicated they wanted an industry consensus, or laws passed concerning privacy policies before their organizations would adopt such policies. Only 14% indicated that they would want their company to pioneer such policy (Westin, 1981). Business organizations indicated at the

time of the study that they would prefer, by a large majority, to have uniform adoption across an industry segment, or have laws or regulations enacted that would provide guidelines for the adoption of policy related to privacy. Several laws and regulations were outlined in the section addressing legislative and regulatory responses to privacy.

Internal Industry Regulation

Business organizations, concerned with potential costs and the impact on profitability, have consistently offered to address privacy concerns through internal or self regulation. Organizations argue that they must respond to market demands relative to privacy concerns or risk the loss of reputation and stature. This position contradicts the opinions and attitudes expressed by business and organizations in Westin's (1981) study. The recent statement by the chief executive of ChoicePoint® (ChoicePoint Asset Company, Alpharetta, GA) regarding the release of information of over 145,000 of its records to illegitimate business fronts echoed the need for industry standards or government regulation (New York Times, 2005). It would appear that business statements are contradictory when expressing preferences addressing industry or government regulation for the protection of personal information. It is difficult to see a logical and systematic progression of business pursuing privacy protections for its customers without there first being problems substantial enough to cause the threat of the loss of business such as in the case of ChoicePoint. It appears that business will address privacy concerns of individuals only when there are significant problems that arise and result in bringing the subject to the publics' attention.

Compliance Costs

Businesses or other organizations have had a difficult time managing regulation and online consumer expectations regarding privacy. Business recognizes the potential benefits and profits that maintaining a positive image with respect to privacy policy can bring about. Some contested estimates have been made of potentially burdensome costs associated with compliance (Hahn, 2001). Reports have been published that speak to the cost of lost customers and revenue associated with marginal or non-compliance (Cyber Dialogue, 2001). As previously discussed, the regulatory response has been fractured and situation-specific. As a result most organizations privacy policies and adherence to those policies are not monitored through legal and regulatory oversight. Direction and decisions are left to the discretion of organizations, which must balance potential risks and benefits to both themselves and the individuals with whom they interact.

Performance

Business response to privacy concerns is primarily reactive, focusing on external threats to their business model (Milberg, Burke, Smith, & Kallman, 1995). Most businesses have chosen an opt-out approach to customer information management. Financial institutions, required to comply with the Gramm-Leach-Bliley Act, were evaluated in a study conducted by The Center for Democracy and Technology (1999). The study found that online mortgage brokers covered by the act were not in compliance with the law while other financial institutions made it difficult for customers to avoid secondary uses of their personal information. The focus on the part of the financial institutions was nominal compliance, offering individuals little or no control,

essentially creating barriers and making it difficult for individuals to maintain control over personal information. It may be assumed that in the four years since these findings were presented that businesses would have made progress on improving their performance. Unfortunately, for many users and customers, the impression of higher risk related to marginal compliance may have already done significant damage to the reputations of online organizations, and more significantly to the reputation of the online environment as a whole.

Factors Impacting Privacy Concern

The situations, environment, and various factors described in the previous sections highlight the complexity and resulting difficulties individuals face when dealing with the concept of privacy. It is evident that there are a number of factors that have the capacity to contribute to an individual's perception of the privacy environment in a general sense. The prior sections laid out only a portion of the aspects of the privacy environment that may impact privacy perceptions. There are also a number of personality characteristics that relate to, and have an impact on the nature of an individual's response to various facets of privacy. This study is designed to evaluate a number of personality characteristics outside the realm of online privacy in order to appraise responses in a comparative manner. The personality characteristics incorporated into the survey instrument are General Disclosiveness, Locus of Control, Generalized Trust, and the Risk Orientation, and Risk Propensity.

Disclosure

For the purpose of this study disclosure in online environments is defined as the act of providing and type of personal information. The information provided may or may

not include personal identifiers. Disclosure, often referred to as self-disclosure in literature dealing with interpersonal relationships, is reviewed in a large body of literature and in a variety of disciplines that deal primarily with social and interpersonal relationships and may include various degrees of intimacy. Petronio (2002) supports a view that disclosure does not necessarily seek social or interpersonal relationships or intimacy as a goal. This study draws upon this distinction for the purpose of evaluating the characteristic behavior. As part of Petronio's Communication Privacy Management theory disclosure is viewed simply as a function of revealing private information. Private information is by its nature personal, and disclosure generally implies, but is not restricted to, the intent on the part of the individual to reveal. Business research has explored the construct in order to help understand consumer behavior related to marketing. Concerns about privacy are an influential element impacting the functionality of the growing mass of electronically collected and stored personal information.

Anonymous disclosure, in and of itself, does not constitute a potential threat to privacy for an individual, not unless the information can be linked to that individual. That is a caveat to the perceived safety posed by anonymous information. Individuals might believe that since anonymous disclosure does not contain personal identifiers, it is of little or no concern in situations where they self-disclose without identifying themselves. This is not necessarily the case. New data analysis techniques that use data aggregation and triangulation, along with techniques used to track online activities such as the use of cookies, allow companies to profile individuals using data that was believed to be anonymous by the individual who generated it. Because this type of data aggregation or triangulation is being used to profile individuals' anonymous information,

it is becoming a more significant concern for those sensitive to the release of personal information.

Online businesses have become acutely aware of the potential importance of disclosure. Over the last decade companies have chanted the mantra of customer relationship management. Companies sought to learn as much as possible about current or potential customers in order to improve their understanding of consumer needs and desires. With an improved understanding, business could better serve customers, enhancing effectiveness and profitability. It has also been subsequently demonstrated that computers are effective in eliciting intimate disclosure, albeit in experimental settings (Moon, 2000). One cannot deny that online disclosure has provided benefits to both individuals and organizations, but concerns about privacy and management of personal information have consistently been in the spotlight.

A significant amount of the early business interest in disclosure arose in the area of direct marketing over the last 20 to 30 years. This interest was further stimulated by the emergence of interactive marketing, made possible by technologies associated with the advent of the Internet and World Wide Web. Business is particularly interested in the concept of disclosure as a result of the recent migration of consumers to online environments. As previously described, detailed records of individuals' activities provide a mechanism for developing and refining targeted marketing strategies. The more effectively a business can elicit disclosure and gather detailed information on individuals, the more efficiently business organizations can address each individual customer in the market. Businesses assert that more detailed information about individuals enhance their ability to serve markets and customers more effectively. They

also assert that it provides improved effectiveness by aiding the business in saving marketing costs and reducing public complaints about unwarranted, inappropriate, or unappreciated solicitation.

Consequences of Online Disclosure

Disclosure is a behavior exemplified by an individual sharing private knowledge with another individual or entity. The knowledge being shared by the discloser may or may not be intimate in nature, and may or may not be in public records, but it usually consists of information generally not shared with the public. The act of sharing personal information may have a multitude of objectives, such as establishing or reinforcing a personal relationship, or pursuing some social goal such as attempting to gain the acceptance of a group. Under many circumstances a person chooses to self-disclose for some personal benefit. This type of benefit-driven disclosure is described by Archer (1987) as an “other to self” or “other” orientation in which the individual is specifically attempting to derive some benefit from the disclosure recipient. This behavior is further characterized by Culnan and Armstrong (1999) as a balancing mechanism used by the individual to weigh the risks associated with disclosure, with benefits derived as a result of the disclosure. The individual’s goal of deriving some benefit from disclosure, combined with the desire of online organizations to gather detailed information about individuals, makes disclosive behavior, and motivation to disclose, an important focal point in attempting to understand online behavior.

The online environment presently exists as a veritable ocean of personal information. Much of this information is the result of some sort of relationship between individuals, or between an individual and groups or organizations. The interest in

disclosure in the context of this study lies at the decision point of maintaining privacy or engaging in disclosure. Most individuals are active in the online environment at one time or another and subsequently participate in an online relationship that often results in some form of disclosure. Information shared in the context of an online relationship might deal with health or financial information, personal or other type of intimate history, discussions of relationships with others, political debate or discussion, or any one of a number of other topics. A problem with this type of disclosure, in contrast to a simple face-to-face exchange with another individual, occurs because the disclosure may potentially be stored in a stable form for an indefinite period, and is easily available for future reference by anyone gaining access. The information may subsequently be combined with other information about the individual and used, without authorization or knowledge of that individual, by anyone gaining access. The individual may or may not benefit from this further use of the information. The problem arises from the fact that the individual has lost control over the use of the information that has been collected.

Disclosure may be used to gain social acceptance. Individuals often present themselves to other individuals or groups in a positive manner in order to gain social control. In this sense, and in a sociological context, disclosure is seen as a strategic mechanism used in attempts to attain some level of social control (Derlega & Grzelak, 1979).

Information control constitutes a fundamental element of privacy. In any given situation an individual seeks to control the extent and flow of the release of personal information. As long as individuals can control the nature and extent of disclosure, some level of privacy can be maintained. If another individual or organization gains control

over the amount and type of information released about an individual, privacy is diminished (Derlega et al., 1993). Considering the vast amount of information on individuals being collected and stored, the impact on privacy of uncontrolled releases of personal information becomes obvious.

Measuring Disclosure

In order to perform a comparative analysis investigating privacy concerns and disclosure, it is necessary to gauge an individual's tendency to disclose. Difficulties have been encountered in attempting to assess disclosure. Various instruments have been developed to measure disclosure but have resulted in inconsistent findings with respect to behavior predictability. There have also been difficulties in establishing relationships to other personality characteristics or standardizing an approach to the assessment of disclosure (Berg & Derlega, 1987; Miller & Read, 1987; Tardy, 1988).

It is important to emphasize that the study did not seek to establish or validate any of these facts or findings. In the context of this study, disclosure was examined only as a general disposition or trait of an individual's behavior with respect to disclosing personal information. The study did not attempt to evaluate levels of targeted disclosure, or level of intimacy, environments, or scenarios under which an individual discloses. The study used the measure to determine if the individual is more or less likely to disclose. Miller & Read (1987) proposed a goal-based model of disclosure which may be related to a goal-based model of behavior in online disclosure.

Wheeless (1978) conceptualized a more general individual trait and referred to the construct as General Disclosiveness. Wheeless conceptualized General Disclosiveness as a more general disposition to disclose, unlike self-disclosure, which is

generally a disclosure to a targeted individual. This conceptualization fit well with one of the goals of the study, that of gauging individuals' more general trait-related personality characteristic related to disclosiveness. Disclosiveness also provided a foundation of related research with respect to additional characteristics that were to be assessed.

Control

While a common or explicit definition for the concept of privacy appears unattainable, a familiar theme that emerges in the discussions on privacy is that of control. It becomes apparent in most circumstances that under the auspices of privacy, individuals seek to control information about, and physical access to themselves.

Schoeman (1992) depicts privacy as a control mechanism that prevents social overreaching, that is, control over the individual, physically or psychologically, by another individual or group. Mirroring this concept of control, privacy for the individual, as viewed in the context of disclosure, is a mechanism for controlling personal or intimate relationships (Derlega, Metts, Petronio, & Margulis, 1993; Petronio, 2002). It assists the individual in preventing social overreaching or group control. Privacy allows individuals to present different faces, or personas, for the multitude of roles that each individual must play in the context of everyday social life. In fulfilling these roles, privacy allows them to be independent of, and unencumbered by, preconceived notions others may have, or could have as a result of intimate knowledge. Intimate knowledge of oneself is critical, but that same intimate knowledge could result in reduced effectiveness in any given situation.

Locus of Control

The concept of locus of control relates to individuals' perceptions about the nature of internal or external sources of control in their life. Rotter conceptualized the construct as being two-dimensional, consisting of the perception of a sense of internal control versus control by external forces, that is, the perception of self control over one's life or control by external influences (Levenson, 1981). Levenson extended this concept, not accepting the line of reasoning that apparent external influences or controls are perceived as being unidimensional. She differentiated the external aspect of the construct into separate dimensions and labeled them chance and powerful others. While this differentiation is still concerned with external control, it allows for a segregation of that which is potentially controllable by an individual from that which is not. Locus of control has also been associated with disclosiveness (Wheeless, Erickson, & Behrens, 1986) and as such provides additional collaborative metrics to gauge an individual's underlying personality with respect to these characteristics.

This underlying personality characteristic, a perception about self, others or chance controlling one's life, potentially impacts the individual's privacy attitude or disposition. If one considers what happens during many online sessions, it becomes apparent that the need to make oneself known is required in many circumstances, whether to gain information about something or to participate in some type of activity. While a particular situation may dictate the necessary level of exchange, an underlying behavior moderator such as a belief in control over one's own life may even impact the willingness to participate in the activity.

Levenson's (1981) instrument for evaluating Locus of Control, and her rationale for developing the instrument relate well to the objectives of this study. As Levenson pointed out, Rotter's scale identified an individual's Locus of Control with respect to internality and externality only. The difference in Levenson's approach is the recognition of a potential division in the external Locus of Control construct. The external dimension of Locus of Control is indicative of individuals' perceived power of external forces over events in their lives. Levenson noted a difference in the perception of external power vis à vis her own experiences. The difference was a critical observation that an individual may believe that even though events may be dictated or controlled by external forces, some of those events could be subject to manipulation or influence while others were seen as a result of fate. She believed that even though some individuals may deem they are constrained by forces outside their control, this situation was not necessarily the way things would have to remain. This attitude addresses an individual's state with respect to a current frame of reference, but reinforces an evaluative perception of a more significant internal Locus of Control. This evaluation speaks not only to disclosiveness but also to an individual's state of mind with regard to control of personal information in an online environment.

In the context of online information, the role of control by the individual appears to focus on anxieties regarding various dimensions of privacy concerns explored and validated by Smith et al. (1996). Individuals appear to harbor less concern about personal information intended for a single transaction or encounter but become privacy-sensitive after the fact. This is a logical expectation in view of the previous discussion related to privacy and control. Individuals knowingly participating in online encounters

are presenting themselves as they choose to be perceived. Outside the context of an intentional encounter, individuals continue to seek to gain or maintain control over their information. An organization's or individual's subsequent maintenance and use of information collected about another individual during an online encounter eliminate all semblance of control by the person who initially provided the information.

Privacy concerns about access to one's information in an offline or online context also appears to precipitate a high degree of irritation. This irritation appears to be brought about by unsolicited communications in the form of emails, or by the potential for residual telemarketing or unwanted postal mail. The government, whether at federal, state, or local levels, significantly influences an individual's perception of a need for control. Government agencies have historically released information about individuals in the course of carrying out their obligations. However, many of these releases of personal information have been regarded as violations of privacy that have precipitated legislative and regulatory responses. The government response has traditionally been fragmented.

Generalized Trust

Fukuyama (1995, p. 195) spoke to the core of the relationship between trust and the functioning of the individual in an online environment: "If networks are to be more efficient, however, this will come about only on the basis of a high level of trust …" Network efficiency takes many forms, in terms of economics, data flows, and goal attainment by providers and users alike. Trust, however, operates on two primary levels, technological and personal. Individuals and organizations using networks must have a belief that the network performs as it is intended: they must trust the technology.

Alternatively, individuals must also trust other individuals in the context of the networked environment. In this context the technology becomes a moderator or filter for an interpersonal interaction such as disclosure. The need to be able to trust those with whom one interacts becomes a more important focus for those engaged in online activity as a consequence of the technology intermediating the ability to interact or communicate on a face-to-face basis. The paucity of supporting mechanisms for effective communication in the online environment, such as body language and physical presence, establishes a prominent need for trusting those one interacts with in online environments. Essentially, online environments strip away many of the supporting mechanisms that aid the ability to establish trusting relationships. If an individual has a reduced inclination to trust others, online environments will present additional barriers for the individual.

Risk

Risk comes in many forms and privacy provides a shield from many types of risk. Somewhat like the concept of control, a common theme of the privacy literature appears to focus on fear of the unknown and a sense of vulnerability (Petronio, 2002; Solove, 2002). Surveys of individuals have confirmed a primary preoccupation with the uncertainties involved in the release of personal information. Individuals are not fully informed about how their information will be used after it is initially provided. Studies have also shown that in the context of providing personal information, people are much more inclined to provide anonymous information or provide information of a more general nature such as hobbies or interests. Increased risk is associated with financial information such as credit card or bank account numbers, personal identifiers such as a

social security number, or medical information. These risks are compelling in terms of the loss of fiscal viability, access to credit, social, or health benefits, employment, factors that allow individuals to provide for themselves, their families, and to reasonably function as members of society.

Rubin and Lenard (2002) attempt to dismiss risks associated with unsolicited communications such as email by stating that there is little or no evidence that consumers are harmed by excessive advertising and marketing. Cranor and LaMacchia, (1998), however, point out the excessive irritation experienced by consumers receiving unsolicited commercial email, the cost in terms of wasted time dealing with the unsolicited email, the Federal Trade Commission's efforts to stop spam, and the costs and efforts experienced by ISP's in dealing with the problem. Commission of the European Communities released a study in January 2001 acknowledging a reduction in spam as a result of efforts by U.S. government regulations, technical solutions by ISPs, new trade association guidelines, and an anti-spam counterculture. These findings point to problems caused by unsolicited commercial email, incurring risks in terms of lost time on the part of employers and individuals, and costs that businesses incur in order to control the problem. Rubin and Lenard's analysis is marginally accurate, but the context is so limited that the analysis can offer little or no reassurance for consumers and employers concerned about risks of losing time and money.

There is also the risk of social repression or pressure to conform as a result of data aggregation (Flaherty, 1989; Kang, 1998; Solove, 2001). This risk speaks to the foundations of a democratic society and personal individuality. A significant amount of literature deals with this issue due to its potential impact on individual freedoms.

Risk has also been investigated with respect to trust. Das and Teng (2004) explored this relationship and conceptually linked risk propensity and trust. They asserted that trust by its nature encourages risk taking on the part of the truster with respect to the trustee.

Privacy Dimensions and Personal Information

Smith et al. (1996) developed and tested an evaluation instrument that measures privacy concerns on four dimensions: error, unauthorized secondary use, improper access, and collection. These dimensions relate to areas of concern that individuals assess when considering the concept of privacy and how it relates to their environment.

Westin, working with Louis Harris and Associates in 1995, developed what was then referred to as a privacy segmentation index. They developed a series of questions that estimate the level of privacy concern individuals possess, and associate the level of concern with the typology Westin developed. In recent studies this scale is referred to as a core privacy orientation (Harris Interactive, 2002). Westin's typology consisted of privacy pragmatists, privacy fundamentalists and privacy unconcerned.

Sheehan (2002) developed a user typology categorizing individual privacy concerns into four groups: unconcerned, circumspect, wary, and alarmed. Sheehan pointed out significant limitations in her approach. However, if the analysis is better developed the increased granularity her typology offers may provide additional insight into privacy concerns and online behavior patterns. Even though the enhanced granularity of Sheehan's typology may provide benefits, there is little to indicate that the use of her approach in this study would provide further insight into the findings.

Spiekermann, Gorssklags and Berendt (2001), using multivariate cluster analysis, further segregated privacy pragmatists into profiling averse and identity concerned. This provides enhanced granularity for the evaluation of privacy concerns and typifies a particular type of concern somewhat like the dimensionality Smith et al. (1996) conveyed in their findings. Online profiling and identity theft have become significant focal points for groups and individuals concerned about privacy. An attempt to describe Westin's typology (Harris Interactive, 2002) in terms of a level of concern should prove beneficial in the analyses performed in this study. The studies by Westin, Sheehan, and Spiekermann, et al., addressed the dimensionality of concern levels individuals express in dealing with privacy issues with Westin's approach being the most widely used.

Smith et al. (1996) refined their evaluation instrument, not only through an extensive series of studies and statistical validation, but in the context of nomological validity, a perspective absent in the majority of other studies related to privacy concerns. Nomological validity refers to the ability of a study's findings to predict results in a broader context of constructs. Their study explored two antecedents, previous experiences and news coverage, which they believed might influence privacy concerns. Individuals who believe their privacy has been violated or compromised in some fashion are going to be sensitized to the concept of privacy and consequences related to its perceived loss or violation. News coverage may also influence attitudes significantly. While not as significant as a personal invasion of privacy, reading news accounts of problems others experience dealing with privacy may color the view of those interested enough to be reading about it.

The study conducted by Smith et al. (1996) also examined personality characteristics often associated with privacy. The constructs of trust/distrust, paranoia, and social criticism were examined in an attempt to assess the relationships of theoretically related constructs to the privacy behaviors of individual's. This study expanded the work of Smith et al. by looking at relationships between various additional attitudes and personality constructs related to the sharing of personal information, such as General Disclosiveness, Locus of Control, Risk Orientation, and Risk Propensity in addition to gauging online behavior with respect to disclosure.

Behavior: Actual Use and Disclosure

Much research in the last couple of decades has investigated the relationship between traditional direct marketing and privacy concerns. Phelps, D'Souza, and Nowak (2001) have demonstrated a relationship between an increase in privacy concerns and a decrease in purchases. At issue with research performed such as that by Phelps et al., is the fact that the findings only apply to a limited type of behavior and are not generalizable to the online market.

Spiekermann et al. (2001) point out that past surveys only gauge attitudes, not behavior. Spiekermann et al. confirmed a disparity between privacy concerns and online behavior, presenting findings that indicate people do not behave in a manner consistent with their privacy concerns. The method used by Spiekerman et al. to study privacy concerns was in a controlled environment with a limited sample. This method limits the reliability and validity of their findings.

Summary

This chapter presents a volume of material addressing the nature of privacy, information concerns and management with respect to organizations and individuals, the current information and privacy environments, and a number of theoretical constructs related to privacy or the perception of privacy. A case is presented that brings into question the expectations of individuals with respect to privacy. Privacy expectations may set a stage for conflict between information gatherers and information providers, instilling in the information providers a sense of safety or underlying belief that, as a function of the ways some information is protected, all information is treated equally. This establishes the foundation for the design of this study. The study is designed to empirically address overt concerns and behaviors related to privacy behavior and privacy concerns and supporting theoretical behavioral constructs that offer some perspective as to why individuals respond to the concept of privacy in a manner that seems counterintuitive. The study provides insight into the relationships between the personality traits and the online privacy concerns and behaviors of individuals.

CHAPTER 3

METHODS AND ANALYTICAL APPROACH

Introduction

This study is designed to contribute to an understanding of the nature of individuals' underlying attitudes toward privacy by assessing theoretically related constructs, assessing attitudes and behavior related to privacy in online environments, and subsequently examining the relationship between two theoretically related latent variables. The study will use a survey instrument, the Privacy Disposition Inventory or PDI, which consists of a number of instruments that have been previously developed and tested, and new instruments developed for this particular study. The intent of this study is not to establish cause and effect. The study is designed to extend the work of Smith et al. (1996) and explore personality factors associated with privacy behaviors in conjunction with dimensions of privacy concern. The intent is to investigate the interactions of behaviors and perceptions that may influence online disclosure, and subsequently influence online privacy behaviors and relationships between those seeking personal information and those being asked to provide it.

The analytical approach incorporates factor analysis to assess the contributions of various observed variables to the postulated latent constructs being investigated. Cronbach's α and correlational analysis are used to evaluate reliability and discriminant and convergent validity. Structural equation modeling is used to provide a holistic

simultaneous perspective of the relationship between the postulated latent constructs and the related observed variables being incorporated for their evaluation. Proposed measurement and structural models are presented with the reasoning supporting the analytical approach. The methodology is described along with the sampling technique. The complexity of the proposed survey instrument prescribes that each of the survey sections, and the included instruments, be discussed in detail.

Survey Instrument Overview

This study is designed to evaluate several related constructs. As a consequence, the resulting survey instrument designed for gathering data is a compilation of a number of individual instruments that were developed to test each of the constructs being investigated. The survey instrument for this study, the PDI, contains three primary sections. The first section is intended to gather information related to a proposed latent construct labeled Functional Privacy Orientation. This section is made up of five instruments measuring 10 dimensions on four primary constructs. This section uses instruments to evaluate General Disclosiveness, Locus of Control, Generalized Trust, and Risk Orientation, and Risk Propensity. The second section is designed to gather information related to a proposed latent construct referred to as Online Privacy Orientation. Instruments related to this construct will use the instruments Willingness to Disclose Online, Level of Privacy Concern, Information Management Privacy Concerns, and Reported Online Disclosure. The final section gathers demographic information on each participant. The proposed latent constructs are described in greater detail later in this chapter.

The following sections describe in detail the survey instrument used in the study, the rationale for modifications to various instruments that are incorporated into the survey instrument, and the approach and logic of the new instruments developed for the study.

Evaluation Instruments

As previously stated, the study is principally a relational analysis of two primary latent constructs: Functional Privacy Orientation and Online Privacy Orientation. Evaluation of the latent construct Online Privacy Orientation incorporates two previously developed instruments and two new instruments. Table 1 lists new and previously developed instruments, the number of original dimensions for each instrument, and number of items. The table also shows parenthetically the number of dimensions and items that are incorporated from each instrument for this investigation.

The original plan for using these instruments was to combine dimensions, creating summed scales of related dimensions. After the initial evaluation of the pilot test results, and based on the advice of experts, it was decided to evaluate all instruments' dimensions individually. Appropriate modifications were made to the hypotheses and research questions to reflect these changes.

Table 1
Privacy Disposition Inventory: Instruments, Sources, Dimensions, and Item Count

Instruments	Author(s)	Dimensions Utilized (original)	Total Items Utilized (original)
General Disclosiveness	Wheeless, 1978	3 (5)	20 (31)
Locus of Control	Levenson, 1981	3 (3)	24 (24)
Generalized Trust	Wheeless, 1977	1 (1)	13 (15)
Risk Orientation	Rhormann, 2002	2 (2)	12 (12)
Risk Propensity	Rhormann, 2002	1 (1)	5 (5)
Willingness to Disclose Online	Grams	1 (n/a)	59 (n/a)
Level of Privacy Concern	Westin, 2002	1 (1)	3 (3)
Information Management Privacy Concerns	Smith, Milberg, & Burke, 1996	4 (4)	15 (15)
Reported Online Disclosure	Grams	1 (n/a)	13 (n/a)

The Survey Instrument

Segregating the survey into three primary sections is intentional. The first section of the survey attempts to gather data related to underlying personality characteristics related to privacy before bringing the participants' cognitive focus to the online environment and related experiences. The goal in using this approach is an attempt to minimize the experiential influence of online activities when attempting to explore the underlying personality traits or attitudes that may influence online behavior. Consequently, the first section of the survey intentionally does not contain any reference to online activity or privacy. The individual's responses to items exploring the personality characteristics or attitudes regarding General Disclosiveness, Locus of Control,

Generalized Trust, Risk Orientation, and Risk Propensity are collected in the first section of the instrument.

The second section of the survey instrument has three primary goals. The goals are evaluating various individual experience and attitude characteristics involving online activity, determining general and specific perceptions related to a level of privacy concern. Level of Privacy Concern measures an individuals' general level of privacy concern. Information Management Privacy Concerns address privacy dimensions related to organizational management of personal information. The first discussion will deal with the instruments used to evaluate General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity. This will be followed by a discussion of the instruments used to evaluate Willingness to Disclose Online, Level of Privacy Concern, Information Management Privacy Concerns, and Reported Online Disclosure. Table 2 locates the various instruments described in the following sections in the survey instrument located in Appendix A.

Table 2
Privacy Disposition Inventory Sub-instruments: Location in Survey and Items

Construct Measured	Begins Page	Total Items Utilized(original)	Notes
General Disclosiveness [1]	158	20 (31)	
Locus of Control [2]	160	24 (24)	
Generalized Trust [3]	162	15 (13)	
Risk Orientation [4]	156	12 (14)	2 items added
Risk Propensity [4]	157	5(5)	
Willingness to Disclose Online	166	59 (n/a)	new instrument
Level of Privacy Concern	165	9 (3)	6 items added
Information Management Privacy Concerns [5]	164	15 (15)	scale reversed
Reported Online disclosure	163	13 (n/a)	new instrument

Notes. [1] Copyright 1978 by Lawrence R. Wheeless. Adapted with permission. [2] Copyright 1981 Elsevier. Adapted with permission. [3] Copyright 1977 by the International Communication Association. Adapted with permission. [4]Copyright 2002 by Bernd Rohrmann. Adapted with permission. [5] Copyright 1996 by the Management Information Systems Research Center (MISRC) of the University of Minnesota and the Society for Information Management (SIM). Adapted with permission.

Proposed Latent Constructs

It is important to establish an understanding of the new proposed latent constructs that constitute the primary focus of this investigation. This study is designed to explore the relationships of several observed variables and two primary underlying latent constructs. The focus of this study lies in establishing the nature of the relationship between how people behave toward or with respect to privacy on an everyday basis and the relationship of this basic behavior to online privacy-oriented behavior. In the context of this study fundamental or core privacy behavior is evaluated as a construct identified as the individual's Functional Privacy Orientation. This conceptualization anchors itself in a discussion Petronio (2001) conveyed in dealing with her Communication Privacy Management theory. She contrasted a logical and

functional perspective with respect to her CPM theory. Evolving from her discussion of Baxter and Montgomery's (1996) "unified oppositions" (p. 8) Petronio elaborates on her own CPM theory by asserting that privacy and disclosure are not logical opposites defined as X and not X, that is, something and everything else, but functional opposites defined as X and Y as outlined by Baxter and Montgomery. In the case of unified oppositions, and in the case of this study, the distinction becomes relevant. This simplifies an investigation by conceptualizing the study in terms of a number of manageable focal points. As further illustrated by Baxter and Montgomery (1996, p. 8); "Functionally defined oppositions are easier to study than logically defined oppositions simply because functional polarities reference distinct phenomena." In contrast to Westin's core privacy orientation (2002), which seeks to divide the population into three primary groups based on privacy attitudes, the basis of this study implies a privacy orientation that is dynamic in nature and moderates the related personality or behavioral characteristics of General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity. Hence Functional Privacy Orientation is a behavior pattern based in a constantly fluctuating balance between privacy and factors that exert influence on privacy, persistently moderated and balanced on a dynamic continuum. From this perspective, outside of extreme cases, an individual's behavior cannot be classified as private or not private, or in the case of Westin's core privacy orientation as three distinct categorizations. Instead this behavior should be viewed as a dynamically moderated balance or interface between what is deemed private and the appropriate individually and dynamically synthesized corresponding level of openness. Hence an individual's Functional Privacy Orientation is indicative of, or influences characteristic

behaviors, and is a function of indicator factors including General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity. These four factors cannot be considered an exhaustive inventory of indicators for individuals' Functional Privacy Orientation. Deeper analyses outside the context of this study would likely confirm these constructs as primary indicators, in addition to other theoretically supported and related constructs.

A second hypothesized latent construct is referred to as Online Privacy Orientation. In addition to being influenced by Functional Privacy Orientation, Online Privacy Orientation is also internally regulated by the individual, incorporating factors related to underlying concerns related to personal information that is released, or provided by individuals to Web sites or companies in online environments. These influences are reflected by a measure of an individual's Willingness to Disclose Online, Level of Privacy Concern, Information Management Privacy Concerns and Reported Online Disclosure. Unlike prior studies (Spiekermann et al., 2001; White, 1999) which sought to understand differences in terms of preferences and actual behavior, this study looks beneath overt behavior and professed attitudes of the individual to assess online behavior in terms of the underlying individual personality. This is a significantly different perspective used to explore the individual's online behavior.

Both of these postulated latent constructs, are based on strong theoretical foundations. In the case of the individual's Functional Privacy Orientation each of the reflective indicators being evaluated provides insight and measurement for attitudes and personality characteristics influencing privacy orientation. With respect to Online Privacy

Orientation, the indicator variables will contribute to a more thorough understanding of the differential impact and the dynamics related to online behavior.

General Disclosiveness

Disclosure, more frequently referred to in the literature as self-disclosure, has a significant investigative history. As a result, several instruments were evaluated as possible candidates to evaluate the construct. Tardy's (1988) chapter on self-disclosure provided an excellent overview of various instruments along with evaluations related to validity and reliability. In addition to the instrument used in the study, other instruments that were considered include Jourard's (1971) Self-disclosure Scale and Chelune's (1976) Self-Disclosure Situations Survey. Considerations for selection included reliability and validity, length of instrument, and participants being evaluated. Based on these criteria, disclosiveness will be evaluated using Wheeless' (1978) Revised Self-Disclosure Scale or RSDS. The instrument was designed to evaluate the dimensions associated with self-disclosure. Tardy (1988) characterized some of the questions in earlier work on this instrument (Wheeless & Grotz, 1976) as being relationship oriented. Wheeless (1978) modified the instrument in his later work and indicated that by generalizing the disclosure target to people in general it could be used to evaluate General Disclosiveness, the tendency to disclose to other people in general. Wheeless referred to the RSDS with a general disclosure target as the General Disclosiveness Scale or GDS. The RSDS/GDS contains 31 items relating to five dimensions of disclosure. The five dimensions: intended disclosure, amount, positive-negative, control of depth, and honesty-accuracy, were not all perceived as necessary in the context of this study. Items evaluating intended disclosure were removed because online

disclosure, by virtue of the fact that the individual must actively seek the disclosure target and make a conscious effort to provide information, was not applicable to this study. Current online environments such as that provided in a physical encounter, or as with other technologies such as the telephone, do not provide as rich a communication environment due to limitations of the technologies. As such an individual's disclosure is more of a conscious and directed effort with an absence of the opportunity for non-verbal types of disclosure which may be unintended. Individuals in an online environment intentionally disclose and are aware of what they are disclosing.

Items related to positive-negative disclosure were also removed. This study's focus is on the individual's general disposition to disclose personal information. Individuals desiring to depict themselves in a more positive or negative manner may be relevant to other studies, but in the context of this study the focus is the fundamental predisposition to disclose. The positive or negative character of the disclosure in the context of this study is not deemed relevant. With the exception of these omissions, the scoring will be as per the instrument scoring protocol. The instrument is reported as being both reliable and valid (Graham, 1994; Wheeless, 1978).

Locus of Control

Locus of Control also has a significant investigative background. Rotters Internal-External Locus of Control Scale is one of the most widely used scales for evaluating this construct (Levenson, 1981). As Levenson pointed out, issues have arisen in prior research questioning the unidimensionality of Rotter's external scale. Lefcourt's works (1981, 1991) provided in-depth overviews of available instruments. Many of the instruments reviewed were developed for specific evaluations such as those dealing

with children, parents, health, alcoholism, and marriage to name only a few. The context of this study eliminated the majority of available instruments as a function of these specialized investigative focuses. The instrument selected to evaluate Locus of Control assesses the construct on three dimensions. The dimensions consist of internal control, control by powerful others, and chance. The instrument, developed by Levenson (1981), consists of 24 items with 8 items designated each for the scales. The dimensional scales will be referred to as Locus of Control/chance, Locus of Control/powerful others, and Locus of Control/internal. Participants are requested to respond to each item using a 6-point Likert scale. Scoring was initially performed per instrument guidelines resulting in a total score from 0 to 48 on each dimension. This instrument has been widely tested and is considered reliable and valid.

Generalized Trust

Generalized Trust is evaluated using a scale developed by Wheeless (1977). The instrument was originally developed to evaluate one individual's attitude regarding trust toward another specific individual. The instrument is referred to as the Individualized Trust Scale. In order to use the instrument for the purposes of this study, participants will be asked to focus on people in general instead of any particular individual. The section consists of a 7-point semantic differential scale with 14 items. The original instrument uses 15 items but was modified for the purpose of this study. One item that targeted a specific individual was removed. Another item reflecting an evaluation of another individual's faithfulness is not deemed applicable to this study. One item, secretive/talkative, was added to support the item confidential/divulging, which Wheeless (1978) reported had failed to load in a prior factor analysis. Polarities

on several items are reversed to help negate response bias as is outlined by Wheeless (1978) in his discussion of the original instrument. Items with reversed polarity are reverse coded before summing the scores. The individual's score can range from 14 to 98.

Risk Orientation

Risk will be evaluated on three dimensions using two instruments developed by Rhormann (2002). The first instrument, the Risk Orientations Questionnaire, consists of 12 statements developed by Rhormann to measure two dimensions of the factor Risk Orientation referred to as general risk orientation and cautiousness. The two dimensions will be referred to as Risk Orientation/cautiousness and Risk Orientation/propensity. Two additional statements developed for this study have been added for a total of 14 statements. Per instrument use guidelines, participants use a 7-point Likert scale to respond to each statement. This instrument is designed to evaluate two dimensions, general risk propensity and cautiousness. The two new statements will be analyzed for their contribution to measuring the construct of general risk propensity. Six of the 12 statements developed by Rhormann are used to evaluate the dimension of cautiousness. The remaining six statements attempt to measure cautiousness and were originally designed to demonstrate an inverse relationship to risk propensity. The author of the instrument hypothesized a two factor structure with an inverse relationship.

Upon review of the items related to cautiousness, it appeared that the context of the wording of the items referred to careful and planning type characteristics of an individual rather than a cautiousness characteristic. Reverse coding of the cautiousness

items resulted in an interpretation of the responses in terms of carelessness, more appropriately related to the verbiage used for the dimension associated with risk propensity, the second dimension measured in this particular instrument. Based on this perspective, items related to cautiousness are reverse coded with the intention of examining the dimensionality in terms of a complimentary relationship as opposed to an inverse relationship. This change resulted in the instrument's dimension being changed to Risk Orientation/carelessness.

The remaining five statements that make up the second instrument, the Risk Propensity questionnaire, evaluate the propensity to take risks in given situations using a 10-point Likert scale. This instrument is subsequently referred to as Risk Propensity.

Scoring for each dimension, as outlined in Rhormann's work, are not used. Risk orientation scores will be summed to provide a net risk orientation score ranging from 6 to 42. Carelessness scores are to be summed to provide a net score ranging from 6 to 42. Risk propensity is summed yielding an overall Risk Propensity score ranging from 5 to 50.

Willingness to Disclose Online

Willingness to Disclose Online will be evaluated using an instrument developed specifically for this project. The instrument consists of 8 categories and 59 items. A scenario depicting a situation in which survey participants would want to participate is presented. The scenario indicates that the activity or service in which participants want to take part will require the disclosure of personal information in order to receive a benefit being offered. This is a common scenario in an online environment. Participants are presented with the list of 59 items and asked to mark the item yes if they would be

willing to provide the information online and no if they would not. If the information does not apply to them, they are offered a not applicable (N/A) choice. The options are grouped into eight sections labeled contact information, likes and dislikes, spouse's information, children's information, personal information, medical information, identification information, and employment information. Specific instructions in the heading of each section bring to the attention of participants groups of items that may not be applicable to them, such as items related to children that they do not have, and indicate they are to skip the section.

Unlike prior studies (Spiekermann, 2001; White, 1999) that presented participants with a particular situation in which they would have to choose whether to disclose or not, this instrument allows the participants to place themselves in their "own" situation. It is hoped that by deemphasizing the specific circumstances, such as those used in prior studies that the participants will be less cognitively challenged or distracted by attempting to interpret a situation or scenario and more inclined to reveal their underlying proclivities with respect to disclosing in online environments.

Level of Privacy Concern

Beginning in 1995 Westin, working with Louis Harris and Associates, developed a simple set of three statements to categorize an individual's level of privacy concern. This instrument has provided consistent results over a period of several years. This instrument provides a benchmark for categorizing an individual's level of privacy concern that should provide some measure of convergent validity with respect to the level of concern reflected in the results provided by the instrument developed by Smith et al. (1996). In the context of this study this index is used to evaluate an individual's

level of concern when dealing with situations involving decisions related to online privacy. This is not consistent with prior use of the metric. Westin's characterization of providing three categories depicting levels of an individual's level of privacy concern was not deemed suitable for the purpose of this study. The same statements will be used instead to capture the individual's more general level of concern. As such, the method used by Westin for characterizing responses will not be used. One of the items will be reverse coded such that summing all three items will provide a total score indicating a level of concern. Using this scoring method will result in scores ranging from 3 to 21.

The method incorporated to determine an individual's level of privacy concern consists of a series of three statements. This instrument was initially referred to as the privacy segmentation index, and in later studies as the core privacy orientation (Harris Interactive, 2002). This approach for determining a privacy orientation has been used in a number of surveys since 1995. It has been utilized in both academic and business environments to typify privacy attitudes and widely used in both scholarly and business publications. The method has not been statistically validated, but appears to provide consistent, repeatable results. While the approach used traditionally is not being incorporated, it is anticipated that an underlying measure of a level of concern is consistent with its design intent.

There are potential problems in having only three items defining an underlying attitude. Consequently four additional items were developed and added to this instrument, which are presented to the participant in the same section of the PDI, that will attempt to enhance the measurement of an individual's level of concern. The items

will be subjected to factor analysis to determine the contribution of each item and total variance extracted.

This index has been used widely since 1995 to gauge the level of an individual's privacy concern. This is the first known study that will evaluate the measure statistically and subsequently attempt to evaluate the relationship between Westin's levels of concern and the levels of concern associated with the dimensions developed by Smith et al. (1996). The opportunity also presents itself for future analysis seeking to develop a more complete picture of the focus of concerns of particular individuals that express a high level of privacy concern. The design of the study provides a comparative analysis of an overall level of concern with a dimensional view relative to a one dimensional generalized level of privacy concern. An analysis of this nature is intended to indicate if privacy concerns, and which individual dimensions of privacy concern, are the focus of participants with a given level of concern reflected by the factor Online Privacy Orientation.

Information Management Privacy Concerns

Individuals' concerns about organizational management of personal information are evaluated using an instrument containing a series of statements developed and validated by Smith et al. (1996).

The instrument Smith et al. (1996) developed, tested, and validated investigates four dimensions of concerns related to organizational management of personal information that confronts an individual when dealing with privacy issues. The four dimensions that were recognized and validated are error, improper access, unauthorized secondary use, and collection. This instrument will subsequently be

referred to as Information Management Privacy Concerns/errors, Information Management Privacy Concerns/improper access, Information Management Privacy Concerns/unauthorized secondary use, and Information Management Privacy Concerns/collection. The polarity of the Likert scale is reversed for this study. The change was made with the intent to alternate scales throughout the survey instrument to avoid between-instrument response bias. Scores will be reverse coded prior to evaluation. Scoring of the privacy dimension instrument consists of a summed total for each dimension resulting in individual scores for each scale ranging from 3 to 28. The instrument was originally designed such that a higher score indicates a higher level of concern.

Reported Online Disclosure

The instrument developed for this study that is essentially a self-report of online disclosure is referred to as Reported Online Disclosure. It consists of 13 statements, 12 of which are to be answered either true or false. The first statement asks participants to indicate if they have ever provided personal information online. If they indicate they have never provided information online they are directed to the next section of the instrument, skipping the 12 statements related to online disclosure. A non-traditional approach was taken with the 12 statements dealing with online disclosure. Prior studies have used various methods to assess information that individuals provide online, either directly or through some type of activity such as logging, self-report of actual activity, browser tracking, or laboratory situations which provide the investigator the opportunity to observe behavior in an artificial environment. A brief explanation of my approach follows.

There are a number of issues associated with attempting to ascertain a level of disclosure in a virtual or online environment. One issue that prevents reliable measures is the fact that online environments in which individuals choose to disclose are generally isolated from direct observation. As a consequence, technologies such as logging or tracking act as communication mediators and may or may not provide an accurate picture or valid and reliable results. Those researchers that have attempted to observe disclosure in laboratory environments create situations that are simulated or artificial by design (Spiekermann, 2001; White, 1999) and are not conducive to natural behavior. Other issues arise with respect to self-report by individuals of previous online disclosure experiences. Not only is the experience colored by time and impressions related to the event, results are also influenced by the ability of the individual to accurately recall the experience.

Reported Online Disclosure is designed to address these issues to some degree and to complement the Willingness to Disclose Online instrument. The instrument accomplishes this by providing a mechanism that allows participants to relate a willingness or reluctance to disclose during their last experience, while at the same time attempting to gauge a degree of disclosure. This is accomplished by incorporating a dichotomous response to 12 statements. This frees the participant from the challenge of remembering specific items and yet allows an evaluation of a natural situation involving online disclosure. This is not to say that the instrument does not have potential issues. It still depends on participant recall of the event and all the associated influence that time and events interject between the event and reporting of the event. Scores are summed, providing a raw score of -7 to +8.

Demographics

In addition to the survey segments described above, a series of questions are asked in the demographics section of the instrument to gauge the individual's level of online activity and experience. The demographics being collected are equivalent to those collected in prior studies. In addition to demographics that are traditionally collected, there are also questions related to prior online experiences. These questions relate to overall computer and online experience in addition to what I will refer to as personal information sensitization events. With the continued growth in the abuse of personal information, such as that experienced from credit card fraud or identity theft, it is felt that some indicators of exposure to these types of abuse would be appropriate. Respondents are asked if they have ever been victims of fraud, or if they believed that any company has ever used their personal information without permission in a way they felt is inappropriate. No specification is requested as to whether it is online or offline since any perceived violation of this type will have the same effect. With the likely impact life events of this nature could potentially have on responses, particularly in the context of this study, I felt it is important to know if such occurrences had taken place. This information is intended to provide additional insight and may be necessary in analyzing responses. Because of the potential impact an event of this nature could impart, it has the potential to be a confounding influence during analysis. Because the respondents will provide this insight into their perceived violations of privacy, the opportunity will be available to deal with it if appropriate. Appendix A contains a copy of the final instrument used for the study.

The Study Population

The population for this study is adults over the age of 18. The sample for this study came from volunteer participants solicited using either email or a solicitation letter. A sample solicitation letter is contained in Appendix E.

For the purpose of this study the primary sample consists of student volunteers from a community college. The entire sampling frame is made up of faculty and staff, their spouses and their children over 18, in addition to students. The project is being provided strong support by the President of the college, who agreed to cooperate in encouraging participation. Volunteers are to be solicited using email. Participants will take part in an incentive drawing that awards the winners gift certificates. I sent a communication in the form of an email from the President's office explaining the study and requesting participation. The communication is preceded by a cover letter from the President of the college encouraging participation both on the part of the faculty and staff, and encouraging the faculty to allow the participation of their students.

Students at the community college consist of two primary groups. One group is full-time students, primarily recent high school graduates, intending to acquire a two or four year college degree, or seeking vocational certification. A second group is individuals currently in the workforce attempting to acquire vocational training or professional certification. This group may also be returning to college for a two or four year college degree to improve their working situation or competitiveness in the job market. This distinction may influence responses in that those participants that have already entered the job market will have broader based experiences than those

participants that have not entered the job market. Demographics collected should allow evaluation for this distinction.

Another sample consists of responses from the faculty and staff, and the spouses of the faculty and staff of a Texas middle school.

The sample may be typified as a combination of convenience and purposive sampling techniques. The sample is convenient in that it looks at a population in a particular geographic location, and purposive in that it moves away from a convenience sample of university students typically used in this type of undertaking. The intent of this approach is to enhance external validity, presenting the findings as more generalizable than that of a sample taken from a single convenient university population. Additional participants were solicited from a local private school, and from small business owners using solicitation letters or email.

Research Involving Human Subjects

This research clearly involved the use of human subjects and consequently required the approval of the appropriate oversight organizations at the University of North Texas. A project description along with supporting documentation was submitted to the University of North Texas Institutional Review Board (UNT/IRB) for the necessary reviews and approvals. Copies of the UNT/IRB approval letters, the UNT/IRB approved Research Project Information Sheet are located in Appendix D. The UNT/IRB also requires applicants that intend to conduct research on human subjects to successfully complete the U.S. Department of Health and Human Services, National Institutes of Health Human Participant Protections Education for Research. This training was completed and a copy of the completion certificate is also located in Appendix D.

Analytical Approach

The design and complexity of this study precipitated the need to use a variety of analytical tools and approaches. Not only does the PDI incorporate a number of previously developed instruments requiring a comparative analysis with previous findings, it also incorporates newly developed instruments that will require analysis to substantiate factor structure, reliability, and validity. The measurement models for Functional Privacy Orientation and Online Privacy Orientation also require assessment to determine model fit. Subsequent to these analyses a structural model consisting of two latent variables will be assessed. The only available means of evaluating the relationship between latent variables is by the use of structural equation modeling. Structural equation modeling is a less widely used technique than other univariate and multivariate techniques and calls for further explanation regarding its use.

Structural Equation Modeling

Structural equation modeling (SEM) is known by a variety of names including covariance structure analysis, covariance structure modeling, and latent variable modeling among others (Kline, 1998; Schumacker & Lomax, 1996). Two important concepts become apparent when looking at the various names associated with the method, that of covariance analysis and latent variables.

SEM is an overarching analytical technique. It is a statistical technique encompassing most analytical variations on the general linear model including multiple and multivariate regression, ANOVA, MANOVA, and canonical correlation (Kline, 1998). But unlike traditional multivariate methods that "… are incapable of either assessing or

correcting for measurement error, SEM provides explicit estimates of these parameters." (Byrne, 1998, p. 3).

There are a number of assumptions associated with the use of SEM that are relevant to this particular study. SEM assumes that the data of the endogenous variables are interval. Exogenous variables may be dichotomous or ordinal. In the case of ordinal endogenous variables, data or matrix conditioning programs such as PRELIS provide a modified covariance matrix to enable their use. The central focus of this study, the evaluation of two latent variables, uses interval scales resulting from the summation of responses in instruments developed previously. The new instruments developed to evaluate Online Privacy Orientation use dichotomous scales. The capabilities of SEM and its associated analytical tools effectively address the full spectrum of analytical needs associated with this study.

SEM also permits an evaluation of validity if two or more measures "… of the same latent variable are substantially correlated." (Schumacker & Lomax, 1996, p. 79). This provides an additional method for evaluating the constructs under investigation with respect to validity. SEM also evaluates a full model with all possible relationships being evaluated simultaneously. This alleviates issues such as those associated with attempting regression analysis using a large number of variables and avoids difficulties associated with a determination of the first-order model, which is generally the most significant independent variable. To illustrate, when determining the first-order model, each independent variable is evaluated outside the influence of, or interaction with, other independent variables. In practice, a more mathematically representative model can be produced by changing the independent variable used to develop the first order

equation. This is not to say that the reformulated model is more theoretically sound, but does speak to an issue of the ability to effectively interpret the results. This is an issue that SEM overcomes with simultaneous full model evaluation.

As is the case with this study, most of the social sciences deal with a significant amount of research studying what is referred to as latent factors. Latent factors are those variables that cannot be directly observed but must be evaluated as a function of something that can be measured or observed. Exploratory factor analysis, confirmatory factor analysis, canonical correlation and other methods have traditionally been used to evaluate the findings of research. What these other analytical methods do not impart is an estimation of error and a representation of the relationships of the multiple factors evaluated simultaneously. What is even more critical, as Byrne (1998. p. 4) has pointed out, is that traditional methods of data analyses only allow evaluation based on observed measurements while "…SEM procedures can incorporate both unobserved (i.e. latent) and observed variables." What is possible with SEM is an evaluation not only of the observed variables to the hypothesized latent variables, but the evaluation of all of the factors with respect to each other and the latent constructs simultaneously. The advantages of this approach, in addition to the abilities to handle various sample distributions and variation in measures such as nominal and ordinal data, speak to the benefits and explanatory power of using SEM as a core analytical tool in this study.

With the above described benefits there also comes a number of factors that should be addressed when using SEM. Even though SEM can be used for exploratory investigations, its primary focus is in confirmatory analyses. This implies that the researcher should have a solid theoretical foundation to support the model being tested.

One of the primary objectives of researchers incorporating SEM should be that of confirming the model using the data and not fitting a model to the data. There are different approaches and considerations for using SEM which include looking at alternative models and equivalent models; however, fitting a model to the data is a recipe for the generation of deficient new theory if the researcher fails to adhere to substantive existing theory.

SEM is more sensitive to various deficiencies in the data. This is to say that data issues such as missing data and outliers can seriously impact results and their interpretation. There are a number of approaches to deal with this issue. Missing data may be addressed using listwise deletion, resulting in observations with missing data being removed. Other methods include replacement based on means, regression and principal components analysis, maximum likelihood, and similar response. Outliers, which can significantly impact results, may also be evaluated in a number of ways, including standard techniques such as histograms, scatter plots, or box plots among others (Schumacker & Lomax, 1996). Many of these capabilities are incorporated into software packages designed to support this type of SEM analysis.

SEM assumes univariate and multivariate normality. It is important that the researcher evaluate normality before conducting model testing. Non-normal distributions do not necessarily rule out the use of the method. SEM software platforms provide the option of using various techniques for normalizing the data such as using mathematical data transforms. Various SEM application platforms also offer estimation methods that do not require normal distributions. The critical factor is the researcher

understands the requirement and subsequent application of appropriate methods to address any problems.

The last significant concern I will discuss is the matter of sample size. There is an ongoing debate regarding appropriate sample sizes for SEM analyses. But it is apparent that due to the nature of the complex relationships being evaluated in the majority of SEM analyses, even simple models should have sample sizes in excess of 100 observations and preferably in excess of several hundred if possible. This study will have in excess of 200 observations. Statistical power will be evaluated using a technique developed by MacCallum, Browne, and Sugawara (1996).

The analytical considerations outlined in this study precipitated the decision to use SEM as the primary analytical technique for the execution of this study. I will now proceed to an explicit discussion of the analytical approach related to this particular study.

Analysis of Observed Variables

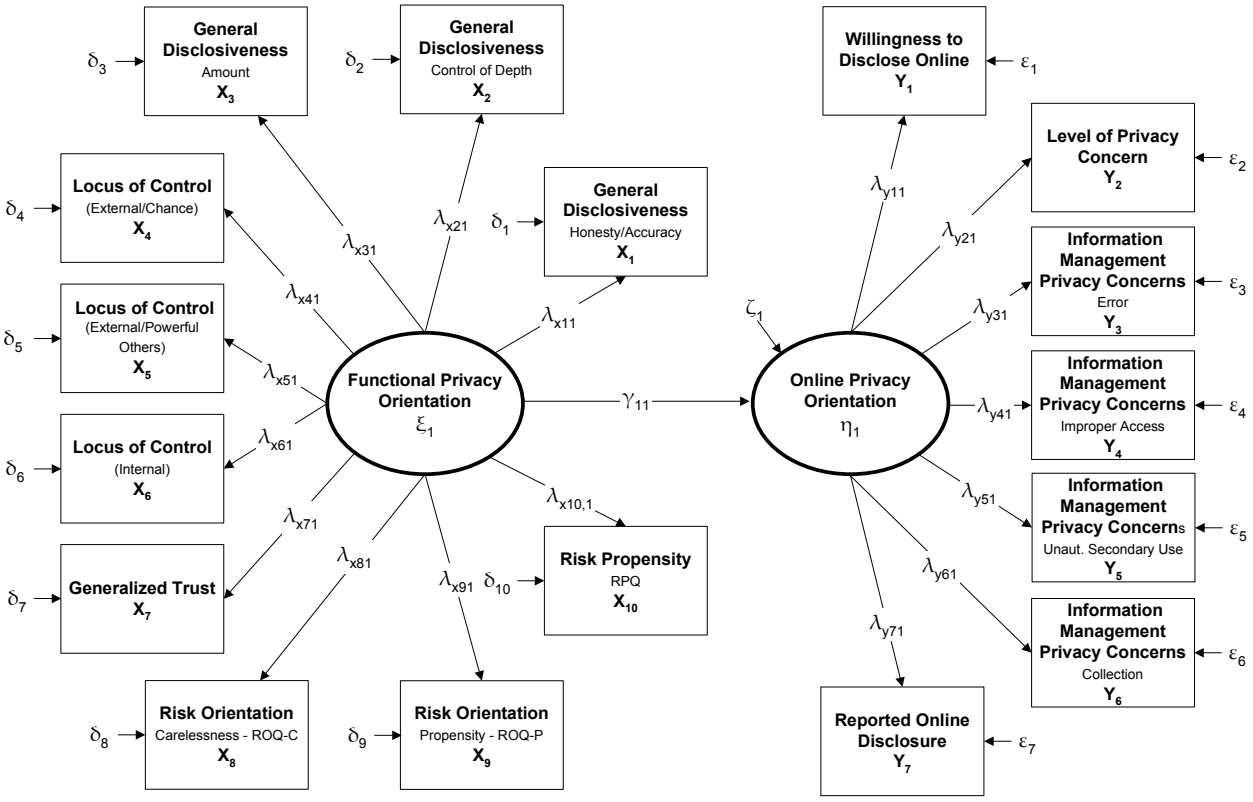
Online Privacy Orientation is operationalized using previously developed instruments designed to evaluate dimensions of privacy concern and levels of privacy concern. In addition to these two instruments, two new instruments discussed previously were developed to evaluate prior online disclosure and the second to evaluate an individual's willingness to provide personal information in an online environment. The first instrument is referred to as Willingness to Disclose Online and consists of 59 items with one postulated factor. The second instrument is Reported Online Disclosure and consists of 13 items with one postulated factor. These instruments will be evaluated using Cronbach's α and corrected item-total correlations.

Risk Orientation and Risk Propensity are measured using two instruments developed by Rhormann (2002). These instruments do not have any formally published results and are evaluated using factor analysis to determine factor structure, loadings and variance extracted. Reliability is assessed using Cronbach's α.

Westin's segmentation index (2002) has not been previously evaluated for either reliability or factor structure. This instrument, Level of Privacy Concern, is evaluated using factor analysis to determine factor structure and loadings. Reliability is assessed using Cronbach's α.

The proposed structural model with measurement models is depicted in Figure 1.

Figure 1. The proposed structural model with measurement models using LISREL notation.



The measurement model for the exogenous independent latent variable, Functional Privacy Orientation, depicts the relationships for the 10 observed variables used for evaluation. The measurement model for the endogenous dependent latent variable, Online Privacy Orientation, illustrates the relationships of the seven observed variables used for evaluation. The measurement model associated with Online Privacy Orientation evaluates types of concerns and level of concern that impact online privacy behavior. Willingness to Disclose Online and Reported Online Disclosure also act as reflective indicators of Online Privacy Orientation. The measurement models are postulated a priori and will be evaluated using confirmatory factor analysis. As discussed previously, the majority of the underlying observed variables consist of measurement instruments intended to operationalize the underlying latent construct. All observed variables consist of constructs theoretically associated with the concept of privacy. Prior to the confirmatory factor analyses the reliability of all previously developed and tested instruments are assessed using Cronbach's α. Reliability results using the current sample will be compared with reliability findings of prior research.

This study is designed to ultimately evaluate the relationship between the two latent constructs Functional Privacy Orientation and Online Privacy Orientation. The nature of the proposed analysis in the full measurement and structural model depicted in Figure 1, which incorporates LISREL notation, visually depicts the relationships being evaluate using structural equation modeling.

Hypothesis Testing

The LISREL™ (Scientific Software International, Inc., Lincolnwood, IL, www.ssicentral.com) notation used in the full structural and measurement model

depicted in Figure 1 allows the hypotheses to be stated in a statistically concise fashion. The proposed hypotheses and their corresponding statistical equivalent can be stated as follows.

H_1: Locus of Control/internal is influenced significantly more than Generalized Trust by Functional Privacy Orientation. Statistically, using LISREL notation: H_0: $\lambda_{x61} \leq \lambda_{x71}$; H_a: $\lambda_{x61} > \lambda_{x71}$.

H_2: Locus of Control/internal is influenced significantly more than either dimension of Risk Orientation by Functional Privacy Orientation. Statistically, using LISREL notation:

H_0: $\lambda_{x61} \leq \lambda_{x91}$; H_a: $\lambda_{x61} > \lambda_{x91}$ and H_0: $\lambda_{x61} \leq \lambda_{x81}$; H_a: $\lambda_{x61} > \lambda_{x81}$.

H_3: The four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection), will load inversely to Online Privacy Orientation with respect to Reported Online Disclosure.

H_4: Online Privacy Orientation is significantly influenced by Functional Privacy Orientation. Statistically, using LISREL notation: H_0: $\gamma_{11} = 0$; H_a: $\gamma_{11} \neq 0$.

T-tests will be used to evaluate the statistical significance of the findings.

Sample Size and Statistical Power

The targeted sample size for this study is 200 to 300 participants. Based on prior studies of the instruments being incorporated, and the number of postulated latent variables being investigated, and a structural model consisting of two latent constructs, this sample size is adequate to attain a minimum statistical power of .80 for the model and will be assessed using the MacCallum, Brown, and Sugawara (1996) method for determining statistical power in a structural model.

Summary

This chapter has provided an overview of the methodological approach used for this study. Instruments, scaling, scoring, and analytical approaches for each part of the study were explained. Justification is provided for the analytical approach. The findings of the study are discussed in chapter 4.

CHAPTER 4

FINDINGS OF THE STUDY

Introduction

This chapter describes the approach used to analyze the data and explain why some of the decisions were made in determining the logical and statistical approaches used for final assessment of the results. Only the results will be presented in this chapter. Research questions and hypotheses will be addressed with the presentation of the results pertaining to each question or hypothesis. Related discussion and interpretation will be presented in chapter 5.

The approaches adopted for data manipulation and analysis are dictated by the nature of the individual instruments incorporated into the survey, their respective factor structures and reliabilities, and their relationship to the final structural model. Corrected item-total correlations, Cronbach's α, and factor analysis were used to assess individual sections of the survey instrument before assessing the measurement and structural models. The findings for the hypothesized and final models are presented to help guide the reader through the reasoning incorporated in making decisions to modify the initially proposed models. As a consequence of the various instruments and their respective scaling, all results are reported in standardized format. To assist the reader in interpreting various decisions made during the process of evaluating the model the LISREL program output for initial and final measurement models and structural model

are located in Appendix B. Statistical analyses were performed using SAS/STAT® software, Version 8.2 (SAS Institute Inc., Cary, NC, www.sas.com), SPSS software, Version 12.0.1 (SPSS Inc., Chicago, IL, www.spss.com) and LISREL software, Version 8.54.

Data Preparation

Upon examination a number of problems were evident in the data. There were a significant number of missing responses, scores contained zero's and negative numbers, and distributions of the data on some of the scales did not appear to be normally distributed. These problems were addressed prior to assessing the measurement and structural models. The rationale used in determining the appropriate approach to each problem and methods incorporated to deal with the problems are detailed in the following sections.

Missing Values

The survey instrument was complex and relatively long. It was designed to assess a total of 17 different dimensions on 8 primary constructs. The length and complexity almost certainly contributed to a number of answers being left blank or pages being skipped by participants. Listwise deletion and pairwise deletion of missing observations provide two possible methods of dealing with the problem of missing data. Pairwise deletion is not recommended in structural modeling techniques due to significant loss of observations and the possibility of non-positive definite covariance matrices. Listwise deletion for this study would have resulted in a loss of 105 total observations reducing the usable sample to 169, a sample considered small in the analysis of covariance structures.

Based on these considerations LISREL routines were used to impute missing values, exclusive of participant demographics. Imputation was done using raw data at the survey item level. Responses to instruments with all missing values were replaced with the variable series mean. Random missing variables were replaced using LISREL's multiple imputation Estimation Maximization routine. This resulted in a total functional sample of 274 observations. Summative scales were then created for each dimension of the observed variables using the imputed data. Exclusive of initial comparative analysis of reliabilities using the original raw data, all subsequent analysis of the data proceeded using this sample of imputed data. Comparative analysis of reliabilities was performed and is covered in the section addressing reliability of the instruments. This comparison consists of non-imputed raw data and the imputed data, and shows the impact of imputation on reliabilities of the various observed variables.

Data Transformations

The factors Locus of Control/chance, Locus of Control/powerful others, Locus of Control/internal, Online Willingness to Disclose, and Reported Online Disclosure all had zero points or negative numbers, or a combination of both as a result of initial scoring in each of their respective scales. General linear transforms were used to provide all non-zero non-negative scales. These data transforms maintained both rank and interval integrity.

Considerations Regarding Data Distributions

Most estimation methods for structural modeling assume multivariate normality. PRELIS 2, a program developed as a component of LISREL, provides data screening

with respect to data characteristics such as sample distributions. This was the approach used in evaluating data distributions.

A preliminary examination of the variable's histograms indicated several of the variables to be both skewed and kurtotic. A subsequent examination of the LISREL output pertaining to univariate normality confirmed that the majority of the observed variables were significantly skewed and kurtotic ($p < .01$). Based on these results the variables were normalized using the Normal Scores routine provided in LISREL. The normalization procedure available in LISREL is considered a monotonic transformation and maintains the sample means, standard deviations, and rank order of the interval variables (Jöreskog, Sörbom, du Toit, & du Toit, 2001). Table 3 shows the χ^2 and *p* values used to assess skew and kurtosis before and after normalization.

As shown in the table all but three of the factors, Information Management Privacy Concerns/improper access, Information Management Privacy Concerns /unauthorized secondary use, and Reported Online Disclosure, achieved univariate normality, that is, the transformation produced normal Gaussian distributions for the majority of the summed scales. Multivariate normality was again evaluated. Even after LISREL normalization, skew and kurtosis were statistically significant ($p < .01$). This fact was taken into account and weighted least squares estimation, which does not assume multivariate normality, was used for model estimation.

Table 3

Skewness and Kurtosis: χ^2 and p -Value Before and After Normalization.

Instrument: Dimension	χ^2 before Normalization	*p* -Value	χ^2 after Normalization	*p* –Value
General Disclosiveness/honesty	3.983	.136	0.006	.997
General Disclosiveness/depth	4.669	.097	0.017	.992
General Disclosiveness/amount	10.232	.006	0.002	.999
Locus of Control/chance	19.656	.000	0.004	.998
Locus of Control/powerful others	6.394	.041	0.001	.999
Locus of Control/internal	26.232	.000	0.004	.998
Generalized Trust	5.365	.068	0.001	.999
Risk Orientation/carelessness	11.998	.002	0.002	.999
Risk Orientation/propensity	0.040	.980	0.005	.998
Risk Propensity	8.570	.014	0.003	.999
Willingness to Disclose Online	9.261	.010	0.631	.730
Level of Privacy Concern	6.034	.049	0.002	.999
Information Management Privacy Concerns/errors	30.792	.000	5.292	.071
Information Management Privacy Concerns/improper access	153.845	.000	26.755	.000
Information Management Privacy Concerns/unauthorized secondary use	232.886	.000	33.708	.000
Information Management Privacy Concerns/collection	53.860	.000	4.288	.117
Reported Online Disclosure	23.110	.000	37.272	.000

Note. Source was LISREL output of descriptive statistics.

Description of the Sample

The final sample with imputed values consisted of 274 observations. As outlined in the chapter 3, participants were solicited from a number of different sites in an attempt to increase participant variability. The majority of the sample consisted of white

(89%) females (72%). The median age for all participants was 32 years old with a mode of 20 years old. Most participants (81%) have been using a computer for online access for over 3 years, but 72% seldom or never make online purchases. Thirty-eight participants (14%) indicated that they had been the victim of identity theft or fraud and 33% indicated they had knowledge of their personal information being misused in some fashion of which they did not approve.

New Instruments Used in the Study

Two new instruments were designed and incorporated into the study, Online Willingness to Disclose and Reported Online Disclosure. These new instruments were used as reflective indicators of the latent variable Online Privacy Orientation. Three instruments have been used in prior studies but statistical analyses have not been formally published. The factor Level of Privacy Concern, a variant of Westin's (2002) core privacy orientation, was used as a reflective indicator for the factor Online Privacy Orientation. The Risk Orientation and Risk Propensity instruments were developed by Rhormann (2002) and were used as reflective indicators of the factor Functional Privacy Orientation. The following sections will discuss the statistical analyses and findings for each of these instruments. Risk instruments will be discussed first, followed by the online disclosure instruments.

Statistical Assessment of the Risk Instruments

A portion of the study attempted to assess the participants personality characteristics associated with risk. Two instruments incorporated in the survey to measure the risk construct have been used in prior studies, but results have not been formally published.

The first instrument used to measure the factor Risk Orientation, consisted of two theoretically related dimensions labeled by its author as Risk Orientation/propensity and Risk Orientation/cautiousness. As discussed in chapter 3, after examination of the items related to the cautiousness dimension it was decided to reverse code these items, creating a complimentary relationship to propensity. This dimension is subsequently referred to as Risk Orientation/carelessness. An additional two items were included related to spontaneity and impulsiveness, characteristics associated with risky behavior. The instruments were analyzed using principal component analysis to ascertain structure and variance extracted. Consequent to the components being theoretically related they were evaluated using oblique promax rotation. Component extraction criteria consisted of a minimum of two items loading at .60 or greater. Items loading at .40 or greater in the rotated solution were retained on the component demonstrating the highest respective loading. This resulted in dropping two items. The respective loading of each item for a two component solution is shown in Table 4. As shown in the table, two components were extracted as hypothesized by the author of the instrument.

Table 4
Risk Orientation: Factor Loadings

Item Number	Component 1	Component 2
1	.84	-.23
2	-.15	.63
4	.54	.33
5	.18	.56
6	.46	.30
7	.03	.64
9	.06	.43
10	.82	-.18
11	-.17	.57
12	.63	-.10
13	-.13	.72
14	.48	.37

Note. Extraction Method: Principal Component Analysis, promax rotation. Component 1 – Risk Orientation/carelessness. Component 2 – Risk Orientation/propensity.

The second instrument, the Risk Propensity Questionnaire, consisted of five items. These items were analyzed using principal component analysis and confirmed the hypothesized single factor structure proposed by the author of the instrument. As shown in Table 5 all items loaded at .60 or greater.

Table 5
Risk Propensity: Factor Loadings

Item Number	Component 1
1	.76
2	.61
3	.63
4	.70
5	.86

Note. Extraction Method: Principal Component Analysis.

Table 6 depicts the number of items examined and retained, and common variance extracted for each component in the two instruments.

Table 6

Risk: Items and Variance Extracted

Instrument and Dimension	Items Examined	Items Retained	Common Variance Extracted
Risk Orientation/carelessness	8	6	28%
Risk Orientation/propensity	6	6	15%
Risk Propensity	5	5	52%

As shown in the table Risk Orientation/propensity was found to account for the least variance. This fact would be taken into consideration during model assessment, in conjunction with additional measures, in evaluating the contribution of Risk Orientation/propensity to the Functional Privacy Orientation measurement model.

Willingness to Disclose Online

When examining the section of the survey used to assess the factor Willingness to Disclose Online several points became obvious. It was noted during data input operations that many of the participants did not skip sections, or otherwise respond appropriately, to sections that did not pertain to them. A comparison was performed based on the participant's reported marital status and items associated with information related to the spouse. Participants indicating they were not married were instructed to skip the section on spousal information. Of those reporting they were not married 17.9% completed the section inappropriately. The same problem occurred in the section dealing with children. A portion (21.2%) of participants indicating they did not have dependent children living with them completed the section dealing with dependent children.

These findings pointed to the fact there was apparent confusion associated with the survey material related to these two sections. Based on these inconsistencies the

sections dealing with spousal and children's information were dropped from consideration for further analysis.

Responses to these optional sections brought into question the reliability of all optional responses; that is, those items outside of the sections dealing with children or spouses but having a not applicable (N/A) response choice. As a consequence, of the 59 items, 23 that provided the optional N/A response were dropped from consideration for further analysis. The remaining 36 items were then subjected to additional analysis.

The remaining 36 item responses were dichotomous in nature. Corrected item-total correlations were used to assess the relationship of the items in the instrument. Those items not having corrected item-total correlations of .40 or greater were eliminated. This resulted in 27 items remaining for further analysis.

Based on the design of the instrument, which grouped items into various categories, two distinct groups of data became evident. One group was made up of common likes and dislikes of the individual such as sports, movies, books, etc. A second group consisted of items pertaining to personal information about the individual related to health, work, education, and other similar items. Based on this distinction each group was analyzed separately, again using corrected item-total correlations. The first group initially consisted of nine items but was subsequently reduced to eight items based on corrected item-total correlations. The items related to what could be considered non-sensitive information. Reliability of this group of responses resulted in Cronbach's α of .968. Based on the small number of items remaining for the group this result appeared unusually high. Considering the low item count and the unusually high reliability measure the frequency distributions of responses were then examined. It

became evident upon examination of the response distributions that there was little variation in the responses. Over 80% of participants responded to all eight items in the same manner. Based on this lack of variability a determination was made that these items provided little differential information about the respondents. Consequently this group of items was dropped from further analysis.

Using the same criteria the remaining 18 items were assessed using corrected item-total correlations. All 18 items exceeded the correlation criteria of .40 and were retained for further analysis. Cronbach's α for these variables was .89, indicating a high degree of internal consistency. An examination of frequency distributions indicated an acceptable degree of variability in the responses, which approximated a normal distribution and did not display the response uniformity encountered in the previously discussed group of non-sensitive items.

Level of Privacy Concern

Statistical evaluation of Westin's privacy statements related to current privacy practices, a factor refered to as Level of Privacy Concern, did not produce statistically significant results. Westin's scale consisted of only three items initially. Taking the number of items originally used, four related items were added to the scale during the design of the instrument. Principal component analysis using promax rotation was used for evaluation to determine factor structure. The criteria for the analysis consisted of a minimum of two items loading at .60 and retaining items with loadings of .40 or larger. The analysis revealed a single component related to the factor Level of Privacy Concern. The items that loaded at .40 or more on the factor Level of Privacy Concern

consisted of two of Westin's statements and two of the new additional statements. Cronbach's α for this factor consisting of four items was .812.

Reported Online Disclosure

The instrument intended to assess online disclosure consisted of one item allowing the participant to indicate if they had ever provided personal information to an online site. Fifty-five of the 274 participants (20%) indicated they had never disclosed personal information online and were directed to the next section of the survey.

The remaining participants answered a series of 12 true/false statements intended to indicate their disclosure of various types of information during their last experience where they wished to acquire something or receive some other type of benefit online. The statements also explored comfort levels associated with disclosing the various types of information. Corrected item-total correlations were evaluated and items not exceeding a corrected item-total correlation of .40 were eliminated. Based on this criterion only three items were retained for further analysis. Cronbach's α for the three remaining items was .63, a marginally acceptable level of internal consistency.

Reliability of Supporting Instruments

Four of the nine instruments being incorporated to evaluate the two postulated latent constructs in this study have been used in prior research reporting reliability. This accounted for 11 of the 17 dimensions being measured. Reliabilities reported in the results of the prior studies are used for comparative analysis of current findings. Table 7 depicts the comparative analysis of data relating to reliabilities. Also included are the reliabilities of the various instruments using imputed data from the current study.

Table 7

Reliability: Cronbach's α; Current study using raw data and imputed data with previously reported results in parentheses

Instruments	Total Items	Cronbach's α (raw data - listwise deletion)	Cronbach's α (imputed data)
General Disclosiveness/honesty	8	.826 (.84*)	.826
General Disclosiveness/depth	5	.671 (.78*)	.668
General Disclosiveness/amount	7	.796 (.82*)	.793
Locus of Control/chance	8	.764 (.73 to .79**)	.762
Locus of Control/powerful others	8	.731 (.72 to .82**)	.729
Locus of Control/internal	8	.533 (.51 to .64**)	.531
Generalized Trust	14	.941 (.92***)	.941
Risk Orientation/carelessness	6	.737 (n/a)	.741
Risk Orientation/propensity	6	.630 (n/a)	.629
Risk Propensity	5	.755 (n/a)	.758
Willingness to Disclose Online	18	.886 (n/a)	.886
Level of Privacy Concern	4	.813 (n/a)	.813
Information Management Privacy Concerns/errors	4	.855 (.84)	.857
Information Management Privacy Concerns/improper access	3	.791 (.75)	.794
Information Management Privacy Concerns/unauthorized secondary use	4	.857 (.80)	.856
Information Management Privacy Concerns/collection	4	.845 (.88)	.846
Reported Online Disclosure	3	.665 (n/a)	.665

Notes. * Using Nunnally's formula equivalent to Cronbach's α (Wheeless, 1978). ** Reported as Kuder-Richardson reliabilities (Levenson, 1981) . ***Reported as a split-half reliability when used as a measure of individualized trust (Wheeless & Grotz, 1977).

Summary Statistics

All subsequent data analysis incorporated the data after all manipulations and assessments outlined in previous sections had been performed. In summary, the data had been imputed and normalized, and necessary summative scale transforms were performed to eliminate zero and negative data points. Instruments with previously unpublished results were evaluated using principal components analysis, Cronbach's α, and corrected item-total correlations where appropriate. As stated previously, interval and rank integrity for each dimension was maintained. The final imputed sample for all statistical tests consisted of 274 observations.

Table 8 shows descriptive statistics for the scales related to Online Privacy Orientation. Table 9 shows descriptive statistics for the scales related to Functional Privacy Orientation.

Table 8

Descriptive Statistics: Summated Variables Related to Online Privacy Orientation[1,2]

Variable Name	Range	Mean	Median	Mode	*SD*	*SE*
OWDSenT – Y_1	18	10.68	11	11	4.60	.28
LevPrivC – Y_2	24	14.96	15	13	5.09	.31
IMPCErr – Y_3	22	22.76	24	28	4.47	.27
IMPCIA – Y_4	17	19.14	21	21	2.94	.18
IMPCUSU – Y_5	24	26.27	28	28	3.42	.21
IMPCCol – Y_6	24	22.87	24	28	4.88	.30
ODTotT – Y_7	6	2.99	3	3	1.93	.12

Notes.[1] Normalized data used in the analysis. [2] (X_{10}); OWDSenT – Online willingness to disclose sensitive information (Y_1); LevPrivC – Level of privacy concern (Y_2); IMPCErr – Information Management Privacy Concerns/error (Y_3); IMPCIA – Information Management Privacy Concerns/improper access (Y_4); IMPCUSU – Information Management Privacy Concerns/unauthorized secondary use (Y_5) ; IMPCCol – Information Management Privacy Concerns/collection (Y_6); ODTotT – Reported Online disclosure (Y_7).

Table 9

Descriptive Statistics: Summated Variables Related to Functional Privacy Orientation[1,2]

Variable Name	Range	Mean	Median	Mode	*SD*	*SE*
GSDHon – X_1	38	38.17	38	38	7.97	.48
GSDCon – X_2	24	16.83	17	14	5.01	.30
GSDAmt – X_3	32	24.96	25	27	7.01	.42
LOCCChar – X_4	47	17.36	17	21	8.44	.51
LOCPOr – X_5	45	18.31	18	12	8.46	.51
LOCIntr – X_6	42	35.04	35	35	6.25	.38
Gtrust – X_7	71	56.41	57	52	14.34	.87
Careless – X_8	35	20.76	20	22	6.23	.38
RiskOPro – X_9	31	27.25	27	25	5.43	.33
RiskPro – X_{10}	45	23.82	24	27	8.94	.54

Notes.[1] Normalized data used in the analysis. [2] GSDHon – General Disclosiveness/honesty & accuracy (X_1); GSDCon – General Disclosiveness/control of depth (X_2); GSDAmt – General Disclosiveness/amount (X_3); LOCChar – Locus of Control/chance (X_4); LOCPOr – Locus of Control/powerful others (X_5);LOCIntr – Locus of Control/internal (X_6); Gtrust – Generalized trust (X_7); Careless – Risk Orientation/carelessness (X_8); RiskOPro – Risk Orientation/propensity (X_9); RiskPro – Risk propensity (X_{10}).

Inter-item Correlations for Measurement Instruments

All summated scales were analyzed using inter-item correlations. Tables 10 and 11 segregate the data into the two groups used to measure Functional Privacy Orientation and Online Privacy Orientation respectively. Table 10 depicts the correlations between the scales used to measure the latent construct Functional Privacy Orientation. These correlations were not the focus of the study but do provide support for convergent validity. The most significant correlation was found in the relationship between X_4 (LOCChar) and X_5 (LOCPOr).

Table 10

Correlations: Variables Related to Functional Privacy Orientation

Variable Name	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}
GSDHon – X_1	1.00									
GSDCon – X_2	-.06	1.00								
GSDAmt – X_3	.17*	.42*	1.00							
LOCCChar – X_4	-.28*	.14	-.12	1.00						
LOCPOr – X_5	-.23*	.17*	-.13	.60*	1.00					
LOCIntr – X_6	.22*	-.01	-.05	-.12	.01	1.00				
Gtrust – X_7	.23*	-.06	-.03	-.31*	-.25*	.19*	1.00			
Careless – X_8	-.14	.05	.13	.01	-.12	.02	-.06	1.00		
RiskPro – X_9	.08	.14	.29*	.03	-.04	-.09	-.20*	.37*	1.00	
RiskOri – X_{10}	.02	.05	.16*	.06	-.02	-.02	-.24*	.43*	.45*	1.00

Note. *Pearson correlation significant at the .01 level (2-tailed). GSDHon – General Disclosiveness, honesty/accuracy (X_1); GSDCon – General Disclosiveness, control of depth (X_2); GSDAmt – General Disclosiveness, amount (X_3); LOCChar – Locus of Control, chance (X_4); LOCPO – Locus of Control, – powerful others (X_5);LOCIntr – Locus of Control, internal (X_6); Gtrust – Generalized trust (X_7); Careless – Carelessness (X_8); RiskPro – Risk propensity (X_9); RiskOri – Risk Orientation (X_{10}).

A high correlation was to be expected based on theory that both dimensions measure individuals' beliefs that outside forces control events in their lives (Levenson, 1981). The three scales used to measure risk were also significantly correlated ($p <$ .01), demonstrating convergent validity.

Examining the correlations in Table 11 all of the dimensions related to Y_3, Y_4, Y_5, and Y_6 Information Management Privacy Concerns were highly correlated. This corresponds to the findings of previous studies (Smith, et al., 1996; Stewart & Segars, 2002).

Table 11

Inter-item Correlations: Variables Related to Online Privacy Orientation

Variable	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7
OWDSenT – Y_1	1.00						
LevPrivC – Y_2	-.15*	1.00					
IMPCErr – Y_3	-.15*	.05	1.00				
IMPCIA – Y_4	-.13	.02	.63*	1.00			
IMPCUSU – Y_5	-.15*	-.06	.57*	.82*	1.00		
IMPCCol – Y_6	-.24*	.17*	.48*	.63*	.56*	1.00	
ODTotT – Y_7	.04	-.22*	-.07	-.01	-.01	-.27*	1.00

Note. *Pearson correlation significant at the .01 level (2-tailed). OWDSenT –Willingness to Disclose Online (Y_1); LevPrivC – Level of Privacy Concern (Y_2) ; IMPCErr – Information Management Privacy Concerns/error (Y_3) ; IMPCIA – Information Management Privacy Concerns/improper access (Y_4); IMPCUSU – Information Management Privacy Concerns/unauthorized secondary use (Y_5); IMPCCol – Information Management Privacy Concerns/collection (Y_6) ; ODTotT – Reported Online disclosure (Y_7).

Examining correlations between constructs associated with Functional Privacy Orientation and Online Privacy Orientation indicated only two significant correlations ($p < .01$). Level of Privacy Concern indicated an inverse correlation with General Disclosiveness/control and Generalized Trust. This would reinforce the premise of the study that the two primary latent constructs, Functional Privacy Orientation and Online Privacy Orientation are measuring different concepts. A number of other significant correlations exist and will be discussed in the closing chapter.

Estimating the Measurement Models

As discussed in the section dealing with data distributions the survey data was not multivariate normal. Weighted least squares estimation used in conjunction with an asymptotic covariance matrix and correlation matrix is expected to provide appropriate estimates of the chi-square and standard errors when data is not multivariate normal (Jöreskog, Sörbom, du Toit, & du Toit, 2001). Based on the observed data distributions,

and the presence of an adequate sample size, this statistical approach was used for estimating both the Functional Privacy Orientation and the Online Disclosiveness measurement models and subsequently the structural model.

Functional Privacy Orientation

Figure 2 depicts the factor loadings and error estimates for the measurement model of the originally hypothesized latent independent construct Functional Privacy Orientation. For the sake of completeness, and to assist the reader in a thorough understanding of the basis for model evaluation, LISREL program output for the initial and final models is located in Appendix B. A number of difficulties became apparent with the measurement model as initially hypothesized. Loading and error estimates indicated a potential problem with Locus of Control/internal. This was somewhat expected based on a low reliability ($\alpha = .53$). Issues were also evident when evaluating the standardized residuals associated with General Disclosiveness/amount, Risk Orientation/carelessness, and Risk Orientation/propensity. Model fit indices for the initially hypothesized model, shown in Table 12, also indicated issues with overall model fit.

It was apparent, based on the fit indices listed in Table 12, and on others indices provided by the LISREL program output that the initially hypothesized measurement model was a poor fit to the data. Theoretically this could lead to the conclusion that Functional Privacy Orientation was mispecified, or that there might be issues with the data or observed variables. Correlations, reliabilities, *t*-values, and standardized residuals were all examined and evaluated for each of the indicator variables.

Figure 2. Functional Privacy Orientation. Initially proposed measurement model with factor loadings and error estimates.

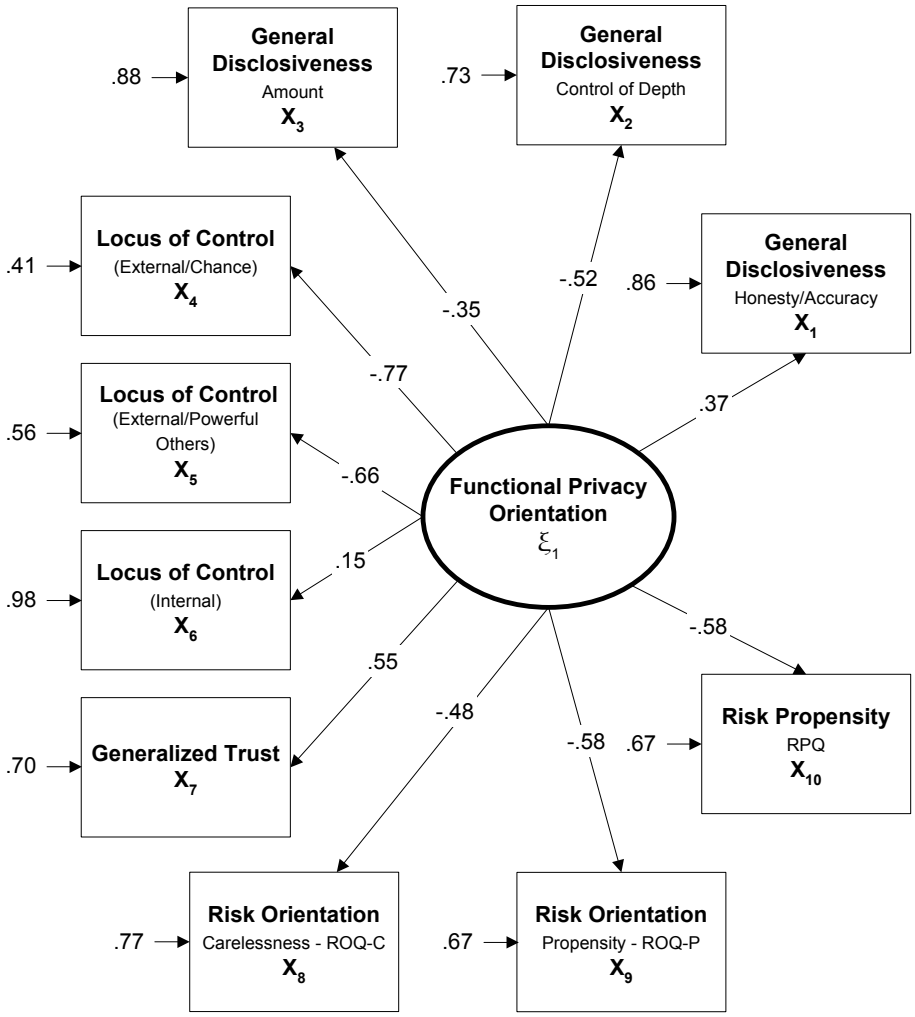


Table 12

Model Fit Indices: Functional Privacy Orientation

Fit Index	Initial Model Values	Final Model Values
χ^2 (df)(*p* value)	$307.43_{(35)(.000)}$	$30.44_{(13)(.004)}$
NCP	272.43	17.44
RMSEA(*p* value)	$.17_{(.000)}$	$.07_{(.140)}$
Standardized RMR	.19	.06
GFI	.91	.99
PGFI	.58	.46
CFI	.62	.95
NFI	.60	.92
Critical N	51.92	249.34

Note. NCP – Non-centrality Parameter. RMSEA – Root Mean Square Error of Approximation. GFI – Goodness of Fit Index. PGFI – Parsimony Goodness of Fit Index. CFI – Comparative Fit Index. NFI – Normed Fit Index.

Based on fit indices and the other considerations listed, that the proposed model required modifications prior to evaluating the structural model. The model modification process was approached iteratively, attempting to isolate the most significant issues and interactions. As various modifications were tested based on different criteria related to modification indices, fit indices, error estimates, and standardized residuals it became apparent there were a number of interactions occurring. Decisions were made based on prior theory and substantive contribution to the model to remove General Disclosiveness/amount, Risk Orientation/carelessness, and Risk Orientation/propensity. Even though Locus of Control/internal exhibited undesirable measurement characteristics it was retained because of its substantive theoretical contribution to the Functional Privacy Orientation measurement model and structural model.

The two most significant modification indices suggested adding an error covariance between General Disclosiveness/control and General

Disclosiveness/amount. This modification was estimated to result in a χ^2 reduction of 81.4 for the model. This was considered prior to removal of General Disclosiveness/amount. The results were not acceptable because fit indices were not substantially improved. This modification also reduced the significance level of the General Disclosiveness/amount loading to a non-significant level ($p > .05$). Based on these considerations the modification was rejected. This finding also indicated a strong interaction between these two variables. Removing General Disclosiveness/amount eliminated the interaction and resulted in an improved χ^2.

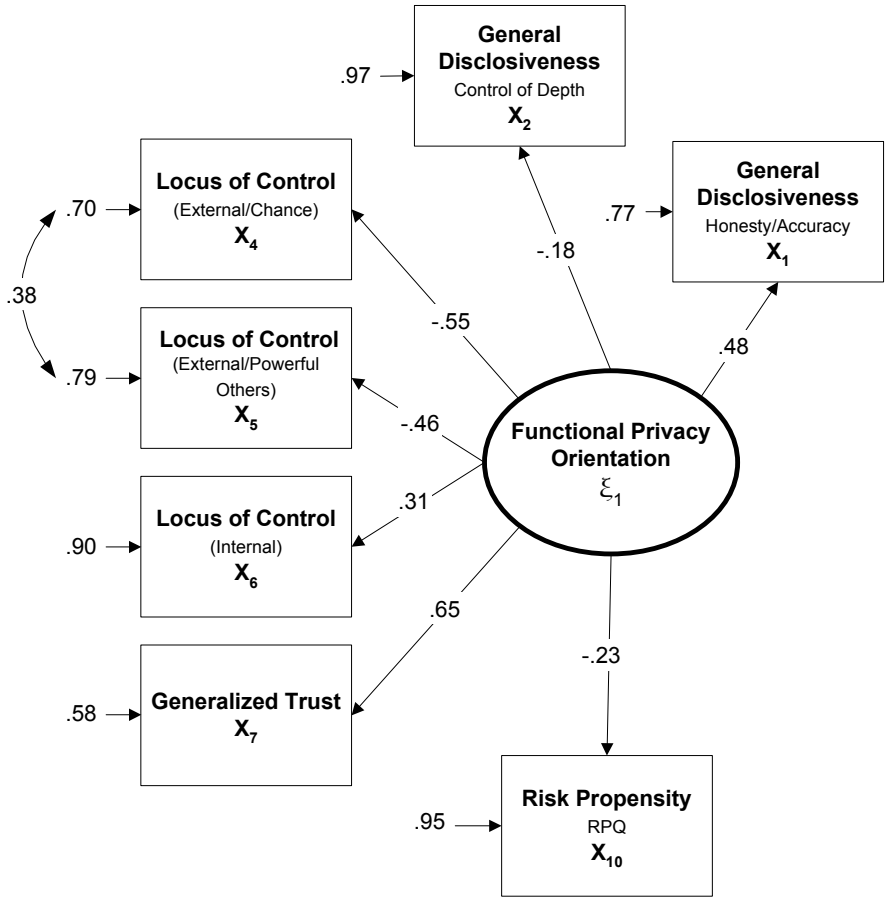
Modification indices also suggested adding an error covariance between Locus of Control/chance and Locus of Control/powerful others. It was estimated to result in a decrease in χ^2 of 58.3. Theoretically these two indicators are related, both measuring the degree of control an individual believes external entities are perceived to exert over life events. The measurement errors were allowed to covary, resulting in the anticipated drop in the χ^2 and improvements in overall model fit.

Risk Orientation/propensity had a low reliability (.63). This fact, combined with the highest standardized residuals, also contributed to a poor fit. Based on these observations Risk Orientation/propensity was removed from the model. This subsequently resulted in the statistical significance of Risk Orientation/carelessness dropping below an acceptable significance level ($p > .05$) and also being removed. Removing these two variables resulted in the model shown in Figure 3 and the related fit indices shown for the final measurement model in Table 2.

The final measurement model for Functional Privacy Orientation, while still exhibiting some marginal measurement characteristics; Root Mean Square Error of

Approximation (*RMSEA*) = .07 and the standardized Root Mean Square Residual (*RMR*) = .059, was considered an acceptable fit. The GFI indicated that 99% of the variance was accounted for between the hypothesized model and the sample data. This modification process resulted in minimizing measurement model modification prior to evaluating the structural model, while attaining a reasonable fit to the data.

Figure 3. Functional Privacy Orientation. Final measurement model proposed for evaluation in structural model with factor loadings and error estimates.



Research Question Related to Functional Privacy Orientation

Research Question 1 is addressed in the context of the findings of the measurement model for Functional Privacy Orientation.

What is the relationship of Functional Privacy Orientation to the multidimensional constructs General Disclosiveness, Locus of Control, and Risk Orientation and to the unidimensional constructs Generalized Trust and Risk Propensity?

This research question was intended to address direction and magnitude of the of the observed variables' relationship to Functional Privacy Orientation. Based on model modifications General Disclosiveness/amount, Risk Orientation/propensity, and Risk Orientation/carelessness were dropped from consideration in the final measurement model for Functional Privacy Orientation and will not be considered in answering this question.

The constructs incorporated into the initial measurement model for Functional Privacy Orientation all indicated statistically significant relationships ($p < .05$). Referring to Figure 2 it can be seen that General Disclosiveness/honesty & accuracy, Locus of Control/internal, and Generalized Trust all loaded positively. The remaining constructs, General Disclosiveness/control, General Disclosiveness/amount, Locus of Control/chance, Locus of Control/powerful others, the two dimensions of Risk Orientation, and Risk Propensity loaded negatively indicating an inverse relationship to Functional Privacy Orientation.

Hypotheses Related to Functional Privacy Orientation

H_1: Locus of Control/Internal is influenced significantly more than Generalized Trust by Functional Privacy Orientation.

The results of the study do not support this hypothesis. Examining the loadings in Figure 3, the final measurement model for Functional Privacy Orientation, indicates that Generalized Trust loaded at .65 while Locus of Control/internal loaded at .31, a

statistically significant difference (t = 4.86, p < .01) of reduced susceptibility to the influence of Functional Privacy Orientation than shown by Generalized Trust.

H_2: Locus of Control/internal is influenced significantly more than either dimension of Risk Orientation by Functional Privacy Orientation.

The results of the study do not support this hypothesis. Due to the fact that the Risk Orientation construct is not included in the final measurement model for Functional Privacy Orientation this hypothesis is addressed by examining the loadings in Figure 2, the initial measurement model for Functional Privacy Orientation. The initial measurement model for Functional Privacy Orientation indicates that Risk Orientation/carelessness loaded at -.48 while Locus of Control/internal loaded at .15, a statistically significant difference (t = -11.05, p < .01). The initial measurement model for Functional Privacy Orientation also indicates that Risk Orientation/propensity loaded at -.58 while Locus of Control/internal loaded at .15, a statistically significant difference (t = -13.15, p < .01). This indicates that Functional Privacy Orientation has an inverse influence on Locus of Control/internal with respect to both dimensions of the Risk Orientation construct but Risk Orientation is influenced significantly more that Locus of Control/internal.

Online Privacy Orientation

Factor loadings and error estimates are depicted in the measurement model for the latent dependent variable Online Privacy Orientation in Figure 4 with fit indices shown in Table 13. Based on a review of the LISREL output, I determined that the majority of the fit indices indicated a marginal but acceptable fit to the data and model modifications were not necessary. The new instruments used in the survey, Willingness

to Disclose Online (Y_1), Level of Privacy Concern (Y_2), and Reported Online Disclosure (Y_7) indicated the lowest factor loadings while those factor loadings associated with the validated instrument Information Management Privacy Concerns (Y_3, Y_4, Y_5, Y_6) indicated the highest loadings. There was an inverse relationship between constructs measuring concerns about information management and privacy and those measuring a willingness to, or actual reported disclosure of personal information in an online environment.

Figure 4. Online Privacy Orientation. Measurement model with factor loadings and error estimates.

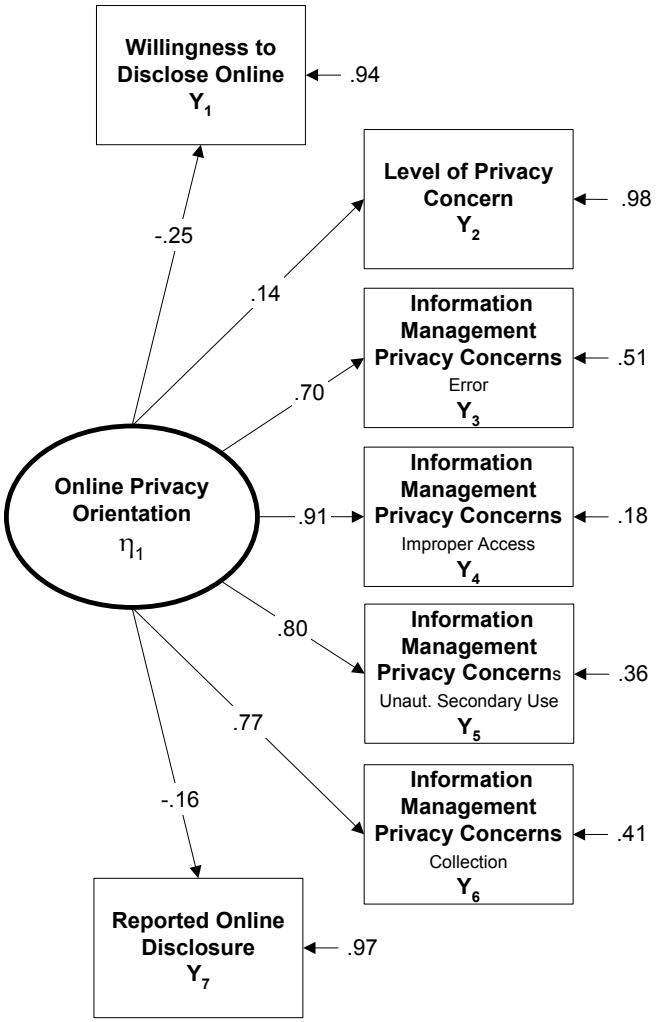


Table 13

Model Fit Indices: Online Privacy Orientation

Fit Index	Final Model Values
χ^2 (df)(*p* value)	$51.07_{(14)(.000)}$
NCP	37.07
$RMSEA_{(p\ value)}$	$.098_{(.003)}$
Standardized RMR	.075
GFI	.98
PGFI	.49
CFI	.96
NFI	.94
Critical N	156.80

Note. NCP – Non-centrality Parameter. RMSEA – Root Mean Square Error of Approximation. GFI – Goodness of Fit Index. AGFI – Adjusted Goodness of Fit Index. PGFI – Parsimonious Goodness of Fit Index. NFI – Normed Fit Index.

Research Question Related to Online Privacy Orientation

Research Question 2 is addressed in the context of the findings of the measurement model for Online Privacy Orientation.

What is the nature of the relationship between the four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection), and Reported Online Disclosure?

Information Management Privacy Concerns are significantly influenced by Online Privacy Orientation and inversely related to Reported Online Disclosure.

Hypothesis Related to Online Privacy Orientation

H_3 addresses the relationship between Reported Online Disclosure and Information Management Privacy Concerns dealing with errors, improper access,

unauthorized secondary use, and collection of personal information and is stated as follows:

> H_3: The four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection), will load inversely to Online Privacy Orientation with respect to Reported Online Disclosure.

This hypothesis was supported in the evaluation of the measurement model for Online Privacy Orientation. As indicated in Figure 4, all dimensions addressing concern about organizational management of personal information loaded positively and Reported Online Disclosure loaded negatively to Online Privacy Orientation. In the measurement model all loadings were statistically significant ($p < .01$) with reliabilities on the measures ranging from .665 for Reported Online Disclosure to .857 on Information Management Privacy Concerns/unauthorized secondary use. Discriminant validity was demonstrated between Reported Online Disclosure and Level of Privacy Concern with a statically significant ($p < .01$) correlation of -.21, indicating an inverse relationship existing between Reported Online Disclosure and Level of Privacy Concern. A statistically significant inverse correlation between Information Management Privacy Concerns/collection and Reported Online Disclosure was also found, further demonstrating discriminant validity with respect to Reported Online Disclosure. These relationships were anticipated. Individuals concerned about their privacy will be less likely to provide information in an online environment and more likely to exhibit a high level of concern associated with information collection practices of organizations.

The measurement model depicting the factor loadings of the dimensions of Information Management Privacy Concerns and Reported Online Disclosure indicates an inverse relationship between the four dimensions of Information Management Privacy Concerns and the single construct Reported Online Disclosure with respect to their loading on Online Privacy Orientation. H_3 is therefore supported. It was also noted that the correlations in Table 11 indicate the only statistically significant ($p < .01$) negative relationship exists between Information Management Privacy Concerns/collection and Reported Online Disclosure.

The Structural Model

The measurement models were then assessed in the context of the full structural model. The initial fit consisting of the final version of Functional Privacy Orientation and Online Privacy Orientation resulted in a moderately good fit to the data. An assessment of a moderately good fit was based on the fit indices shown in Table 14. In assessing the fit of the base structural model it was apparent that the χ^2 was relatively large and that the RMSEA and standardized RMR were outside of acceptable ranges. The LISREL results were examined and based on an assessment of the results it appeared that Level of Privacy Concern and Reported Online Disclosure exhibited a high unique variance and large standardized residuals. Based on these observations of poor fit both Level of Privacy Concern and Reported Online Disclosure were removed from the model. Modification indices in subsequent runs of the model indicated an improved fit by covarying the errors associated with Locus of Control/chance and Locus of Control/powerful others. Modification indices also indicated an error covariance between Information Management Privacy Concerns/collection and Willingness to Disclose

Online. Both of these modifications were made and the resulting model indicated a good fit to the data across the full spectrum of fit indices with the only marginal criteria being that of Critical (N) which slightly exceeded the sample size of the data collected. LISREL program output for the base and final model, which lists the covariance matrix as well as fit indices and matrix related output, is contained in Appendix B. A comparison of select fit indices for the base and final structural models are shown in Table 14.

Factor loadings and the error estimate for the structural model consisting of the latent independent variable Functional Privacy Orientation and the latent dependent variable Online Disclosiveness are depicted in Figure 5.

Figure 5. Structural model with factor loading and error estimate.

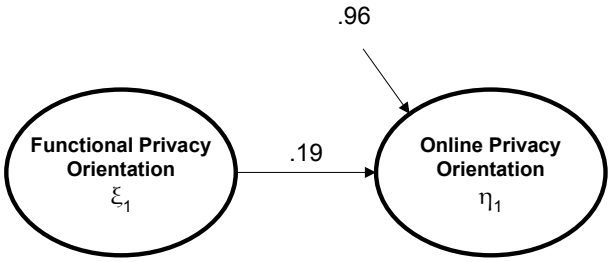


Figure 5 presents only the final structural model, not demonstrating the impact on the various indicator variables of assessing all of the relationships simultaneously. As discussed, further modifications were made to the model based on fit and modification indices. Most significantly Level of Privacy Concern and Reported Online Disclosure were removed from the model. In assessing the measurement models Functional Privacy Orientation and Online Privacy Orientation independently, as depicted in Figure 3 and Figure 4 respectively, they were found to fit the data reasonably well. In the

context of the structural model further issues arose which precipitated the removal of Level of Privacy Concern and Reported Online Disclosure from the final model.

Table 14
Model Fit Indices: Structural Model

Fit Index	Initial Model Values	Final Model Values
χ^2 (df)(*p* value)	$257.97_{(64)(.000)}$	$74.82_{(51)(.017)}$
NCP	193.97	23.82
$RMSEA_{(p\ value)}$	.110	.041
Standardized RMR	.074	.052
GFI	.95	.98
PGFI	.67	.64
CFI	.84	.98
NFI	.80	.94
Critical N	99.65	283.36

Note. NCP – Non-centrality Parameter. RMSEA – Root Mean Square Error of Approximation. Standardized RMR – standardized Root Mean Square Residual. GFI – Goodness of Fit Index. PGFI – Parsimony Goodness of Fit Index. CFI – Comparative Fit Index. NFI – Normed Fit Index.

Statistical problems with Level of Privacy Concern and Reported Online Disclosure had previously been noted. Once these variables could be evaluated in the context of the full model, the problems associated with statistical significance and residuals became significant enough to warrant their removal.

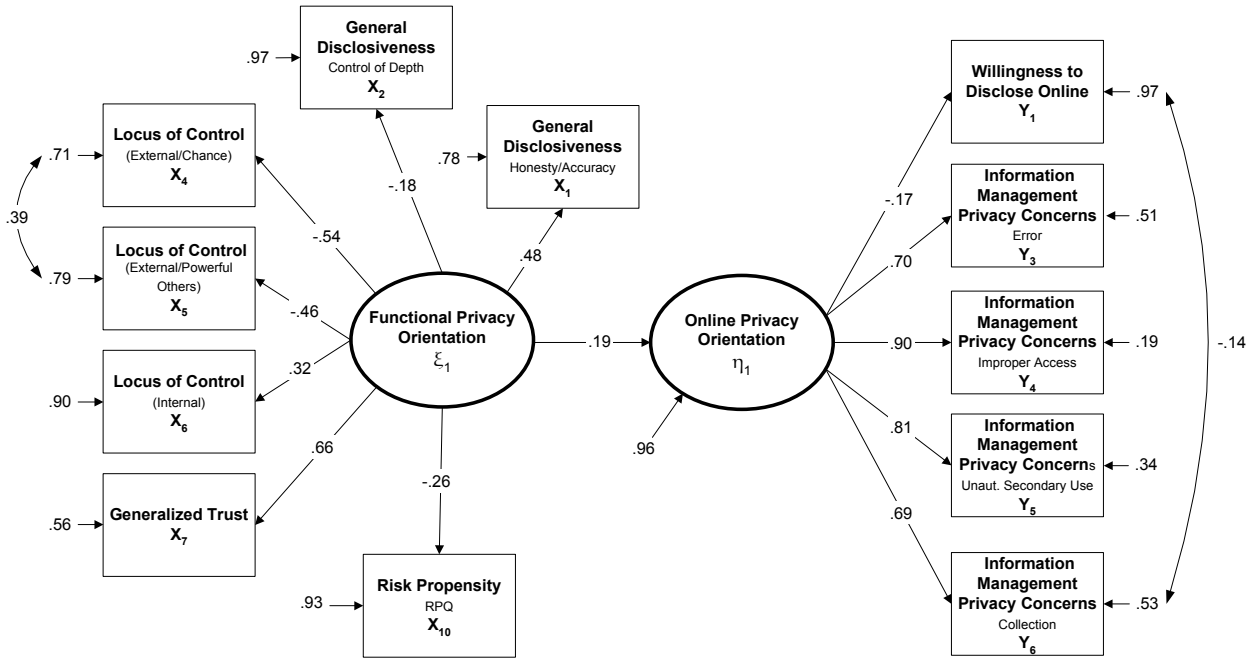
Notably, the full measurement and structural model shows the impact of the interaction of all of the indicator variables when considered as a single model. Several of the loadings and unique variances for the indicator variables changed as a result of the evaluation of all indicator variables simultaneously in the context of the two latent variables. This approach in assessing latent variables allowed for additional refinement of the model through the evaluation of the effects of overall interaction. The final resulting model provides a refined view of the two latent variables, Functional Privacy

Orientation and Online Privacy Orientation, in the context of this study and confirmed suspected issues with two of the indicator variables.

Figure 6 depicts a view of the structural model with measurement models. This illustration accurately depicts not only the modifications made to the Online Privacy Orientation measurement model but also illustrates the impact on the magnitude of the loadings of the observed variables when evaluated in the context of the full model.

Statistical power was calculated for the structural model using a technique developed by MacCallum, Browne, and Sugawara (1996) specifically for statistical power assessment in structural equation models. A SAS routine incorporating RMSEA for both the null and alternate hypotheses, a given significance level ($p < .05$) for the model, sample size, and degrees of freedom yielded a statistical power of .98 for the final model.

Figure 6. The structural model with measurement models depicting structural regression coefficients and error terms.



Research Question Addressed by the Structural Model

The structural model depicted in Figure 5 addresses Research Question 3:

Does Functional Privacy Orientation predict Online Privacy Orientation?

The exogenous latent independent variable Functional Privacy Orientation offers predictive value with respect to Online Privacy Orientation. The residual error associated with the final structural model is large (.96), indicating a potential misspecification or evaluative gap in the approach used to estimate the latent variables. The GFI, a measure of absolute fit indicated that 98% of the variance between the hypothesized model and the sample data was explained. This will be discussed in the closing chapter.

Hypothesis Addressed by the Structural Model

H_4: Online Privacy Orientation is significantly influenced by Functional Privacy Orientation.

Referring to Figure 6 the loading of 0.19 is statistically significant ($t = 2.51$, $p < .05$) and supports H_4. Online Privacy Orientation is significantly influenced by Functional Privacy Orientation.

Summary

chapter 4 has covered the scope of procedures and analyses used in evaluating the data and succinctly presented the factual findings. An interpretive discussion of the findings was neither intended nor attempted. Model modifications were explained. Low reliabilities of some of the instruments indicated issues with respect to their reliability in measuring the intended construct. Direction and magnitude of inter-item correlations indicated both convergent and discriminant validity and supported findings in prior

studies. The research hypotheses and questions were individually addressed, and raised a number of additional questions with respect to the validity and reliability of the study. The implications of the findings will now be discussed in the final chapter.

CHAPTER 5

CONCLUSIONS

Introduction

This chapter discusses the results of this study and its contribution to research in the area of privacy-related information behavior in online environments. The first section provides a synopsis of the significant findings. The following sections describe in more detail the measurement models that define the latent constructs Functional Privacy Orientation and Online Privacy Orientation and the relationship between the latent constructs that constitute the structural model. Methodological limitations are then reviewed. The final sections present theoretical, methodological, and practical implications of the results and offers suggestions for future research.

Overview of the Study

This study was designed to investigate online privacy behaviors and concerns, and their relationship to personality characteristics associated with more generalized privacy-related behavior. Two new latent constructs, Functional Privacy Orientation and Online Privacy Orientation, were proposed in the study. Functional Privacy Orientation, defined in this study as a measure of individuals' generalperception of control over their privacy unrelated to the online environment, was measured using indicator variables General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity, personality characteristics associated with the concept of privacy in the

literature. Online Privacy Orientation, defined in this study as a measure of individuals' perception of control over their privacy in an online environment, was measured using Willingness to Disclose Online, Level of Privacy Concern, Information Management Privacy Concerns, and Reported Online Disclosure as indicator variables.

The majority of the indicator variables reflecting the proposed latent variables have been used in prior research and were integrated into this study with some modifications. Factor analysis, reliability analysis using Cronbach's α, corrected item-total correlations, and inter-item correlations were used to assess new instruments and instruments whose results had not been previously published. Two new instruments, referred to as the Willingness to Disclose Online and Reported Online Disclosure were assessed and are discussed with respect to specific problems.

Modifications to the measurement and structural models were made as discussed in chapter 4. In the final measurement models all indicator variables loaded at significant levels ($p < .05$) to their respective latent variables. The structural model indicated that Functional Privacy Orientation does influence Online Privacy Orientation. Statistically, the structural model demonstrated a significant ($p < .05$) relationship between the exogenous independent latent variable Functional Privacy Orientation and the endogenous dependent latent variable Online Privacy Orientation. The latent variables, while formulated as unidimensional constructs, proved to be bipolar constructs. The measurement models contained both positive and negative loadings from their respective indicator variables. This aspect of the findings will be further discussed.

It is important to emphasize that this study is not about defining the nature of privacy or an attempt to explore all the components that may be used to explore or explain behavior related to privacy. When individuals act, react or behave based on considerations related to privacy, it is important to remember that privacy ". . . can only be understood by reference to norms of behavior" (Post, 1989, p. 969). Drawing from Post's observation, this study examined individuals' traits with respect to information behavior related to privacy in an effort to interpret the influence these traits have on behavior in online environments. Furthermore, it is important to acknowledge again that this study addresses privacy in the context of personality traits and online environments and does not address other aspects of privacy such as physical access, surveillance, autonomy, or social freedom.

The Measurement Models

The measurement models for Functional Privacy Orientation and Online Privacy Orientation provide the basis for interpreting the structural model. The relationships of the various indicator variables are discussed. Problems that arose during the evaluation of the measurement models, and the reasoning used to arrive at the final models are also addressed.

Functional Privacy Orientation

Conceptually, Functional Privacy Orientation is a general model of privacy-related behavior, rooted in individuals' world views. It is composed of their cognitive interpretation of and reaction to their surroundings and life experiences, culminating in their privacy-oriented interactions with the cultural and social environment. Functional Privacy Orientation indicates the degree to which individuals feel they control their

privacy, regardless of how they interpret the concept. In quantitative terms, an increase in Functional Privacy Orientation reflects a perception of increased control. This study presents Functional Privacy Orientation as a latent construct measured by several reflective indicators including individuals' willingness to disclose personal information to others, perception of who or what controls events in their lives, willingness to trust others, and propensity to take risks in various situations.

The originally hypothesized measurement model for Functional Privacy Orientation with loadings and error estimates is shown in Figure 7. Research Question 1 referencing the Functional Privacy Orientation construct asks:

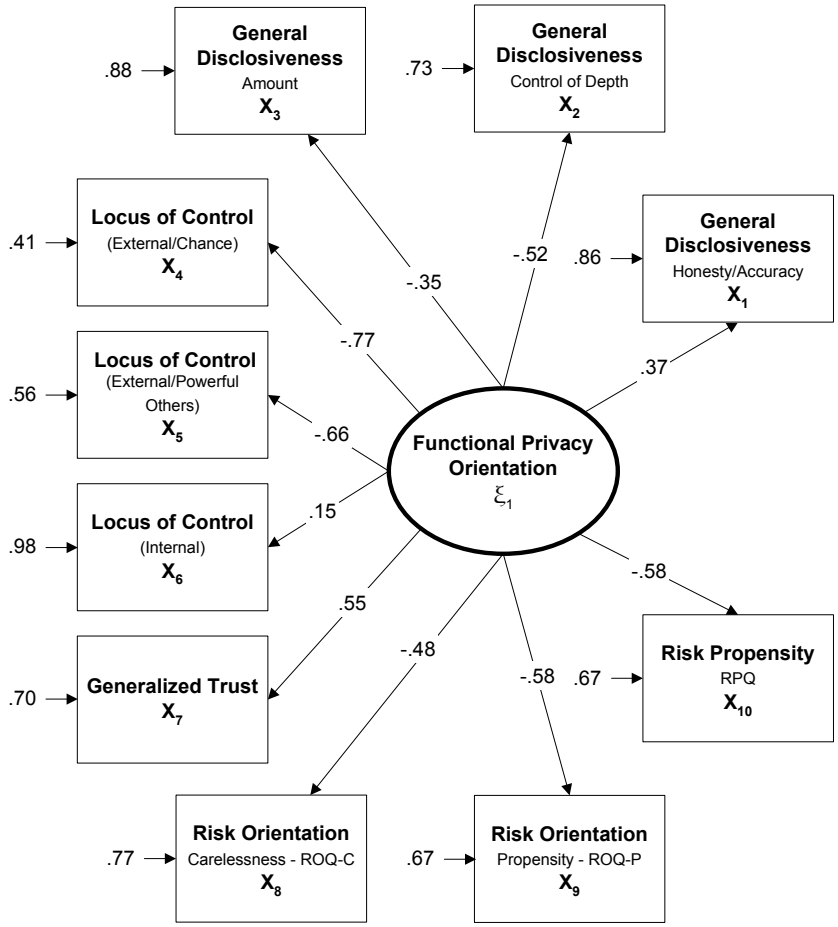
> What is the relationship of Functional Privacy Orientation to the multidimensional constructs General Disclosiveness, Locus of Control, and Risk Orientation and to the unidimensional constructs Generalized Trust and Risk Propensity?

While the model fit was marginal, the results did address the core of this question concerning the fundamental relationships; that is, the magnitude and direction of the indicator variable loadings to Functional Privacy Orientation.

Figure 7 shows that three of the indicator variables, General Disclosiveness/honesty and accuracy, Locus of Control/internal, and Generalized Trust load positively, while the remaining indicator variables, General Disclosiveness/control, General Disclosiveness/amount, Locus of Control/chance, Locus of Control/powerful others, Risk Orientation/carelessness, Risk Orientation/propensity, and Risk Propensity load negatively. All indicator variables are significant ($p < .05$). These results indicate that General Disclosiveness/honesty and accuracy, Locus of Control/internal, and Generalized Trust have an inverse relationship to General Disclosiveness/control,

General Disclosiveness/amount, Locus of Control/chance, Locus of Control/powerful others, Risk Orientation/carelessness, Risk Orientation/propensity, and Risk Propensity with respect to Functional Privacy Orientation. Addressing both positive and negative loadings together in the context of a bipolar factor allows a more specific assessment of the indicator variables with respect to Functional Privacy Orientation.

Figure 7. Loadings and error estimates of indicator variables on originally hypothesized measurement model for Functional Privacy Orientation.



The structural regression coefficients indicate that as Functional Privacy Orientation increases, that is, the more individuals feel they control their privacy and thus the honesty and accuracy of their disclosures, the more they feel they have

personal control over life events, and the more generally trusting they are of others. Conversely, these same individuals do not seek to control the depth or intimacy of their disclosures and are inclined to reduce the amount of their disclosures. They are less inclined to believe that others, or to believe that chance controls life events, or to perceive themselves as careless or likely to take risks. The bipolar nature of this latent construct only begins to reveal the complex behavioral mechanisms that constitute individuals' general privacy behavior.

The marginal model fit of the initial model (see fit indices Table 12, p. 106) of the latent variable Functional Privacy Orientation, presents problems in addressing the following hypotheses:

H_1: Locus of Control/internal is influenced significantly more than Generalized Trust by Functional Privacy Orientation.

H_2: Locus of Control/internal is influenced significantly more than either dimension of Risk Orientation by Functional Privacy Orientation.

Addressing H_1, the structural regression coefficients indicate an inverse relationship between Locus of Control/internal and Generalized Trust. Addressing H_2 the structural regression coefficients indicate an inverse relationship between Locus of Control/internal and the two dimensions of Risk Orientation. The magnitude of the loadings show that Functional Privacy Orientation influences Locus of Control/internal the least of the constructs referred to in these hypotheses. While the initial model addresses H_1 and H_2, that is, the loadings determine that neither H_1 nor H_2 are supported by the findings, the fit of the model requires further consideration.

Several factors had a potentially negative impact on the model fit. Locus of Control/internal had the lowest reliability of all indicator variables (α = .53) and the lowest loading (.15) on Functional Privacy Orientation.

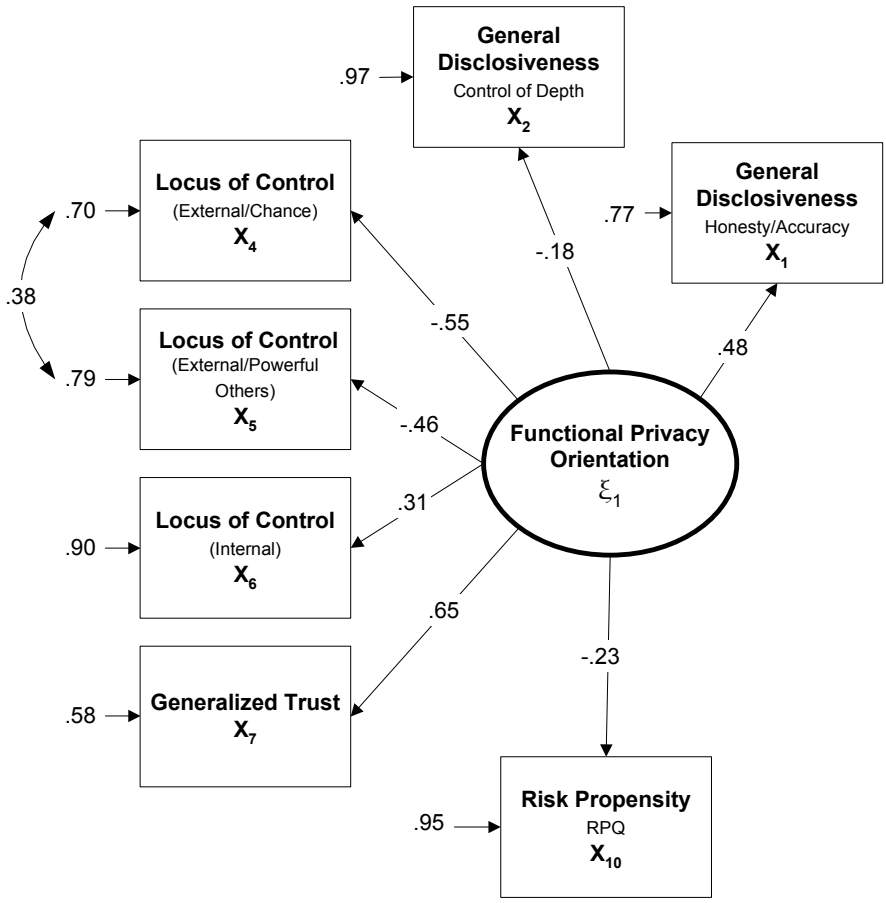
The problem may be the distribution of the data collected for Locus of Control/internal. The LISREL output revealed Locus of Control/internal to be the most highly skewed of the three dimensions measuring Locus of Control. Even though all three dimensions were scaled equivalently the mean of this dimension was significantly higher than that of either Locus of Control/chance or Locus of Control/powerful others (see Table 8, p. 100). This finding indicates that if individuals believe they are in control of events in their lives, their belief is strong. A post hoc confirmatory factor analysis of the Locus of Control data also indicated low loadings on a number of the items for both the internal and chance dimensions, resulting in an overall poor fit to the data.

Theoretically, the chance and powerful others dimensions of Locus Of Control are considered as indicative of individuals who believe that outside influences have control over life events. The internal dimension of Locus of Control is considered indicative of individuals who believe they control events in their lives. While there were difficulties with the reliability of the measure, it did appear to be valid. Inter-item correlations (see Table 10, p. 102) demonstrated convergent validity for Locus of Control/powerful others and Locus of Control/chance. Discriminant validity was demonstrated by the inverse relationship between Locus of Control/chance and Locus of Control/powerful others to Locus of Control/internal. Although reliabilities of the three dimensions were in the range of previous findings, and convergent and discriminant

validity were evident, a measurement problem with the Locus of Control instrument was evident.

The initial model addressed Research Question 1, H_1 and H_2. However, given the measurement problems and fit indices it would be difficult to assess Functional Privacy Orientation in the context of the structural model. Modifications were made to the originally hypothesized model based on the results of the initial analysis. The model resulting from modifications to the initial model is depicted in Figure 8.

Figure 8. Loadings and error estimates of the final model for Functional Privacy Orientation.



Based on modification indices, fit indices, and residuals, General Disclosiveness/amount and the two dimensions of Risk Orientation were removed. Error

estimates of Locus of Control/chance and Locus of Control/powerful others were allowed to covary based on their theoretical relationship and modification indices. The modified model, although showing improved fit, could no longer address all of the relationships referred to in Research Question 1, still did not support H_1, and could no longer address H_2.

Online Privacy Orientation

Conceptually, Online Privacy Orientation is a general model of online privacy-related behavior. Online Privacy Orientation can be defined as a latent construct that indicates the degree to which individuals are inhibited in sharing personal information by concerns about their information privacy in an online environment, regardless of how they interpret the concept of privacy. In quantitative terms, an increase in Online Privacy Orientation reflects an increase in concern about control of personal information in an online environments and a decrease of online disclosive behavior. Online Privacy Orientation is a latent construct measured in this study by several reflective indicators involving individuals' willingness to disclose personal information online, a general level of concern about information privacy, a level of concern about organization's management of personal information, and reported online disclosure.

The measurement model for Online Privacy Orientation addresses Research Question 2:

> What is the nature of the relationship between the four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection), and Reported Online Disclosure?

The measurement model for Online Privacy Orientation also addresses H_3, related to information privacy concerns and online disclosure:

> H_3: The four dimensions of Information Management Privacy Concerns (error, improper access, unauthorized secondary use, and collection), will load inversely to Online Privacy Orientation with respect to Reported Online Disclosure.

The findings of the study supported this hypothesis, but with certain qualifications related to the model fit. The four dimensions of Information Management Privacy Concerns: error, improper access, unauthorized secondary use, and collection have an inverse relationship to Reported Online Disclosure with respect to Online Privacy Orientation. The measurement model for Online Privacy Orientation is depicted in Figure 9.

The loadings and model fit indices (see Table 13, p. 112) indicated that the hypothesized model fit the data well. The RMSEA and the standardized RMR were marginally acceptable at .07 and .06 respectively. Level of Privacy Concern and Reported Online Disclosure had the highest reported unique variance at .98 and .97 respectively, but both variables had statistically significant loadings ($p < .05$). Because a reasonably good fit was obtained prior to evaluating the structural model, no modifications were made to the initial model.

Figure 9. Loadings and error estimates of the measurement model for Online Privacy Orientation.

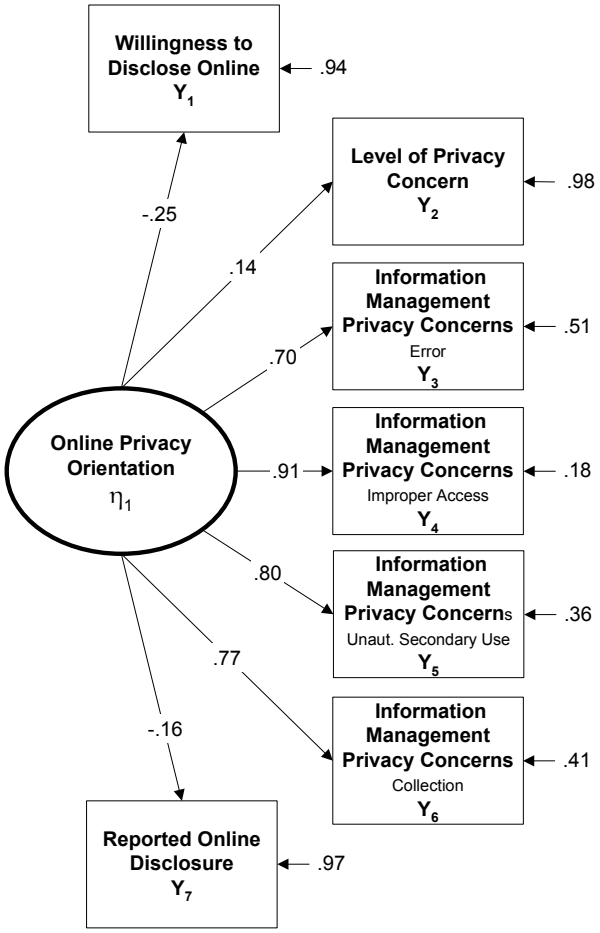


Table 15 shows inter-item correlations related to Online Privacy Orientation. A number of inter-item correlations related to Online Privacy Orientation that merit further discussion.

Table 15

Inter-item Correlations: Variables Related to Online Privacy Orientation

Variable	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7
OWDSenT – Y_1	1.00						
LevPrivC – Y_2	-.15*	1.00					
IMPCErr – Y_3	-.15*	.05	1.00				
IMPCIA – Y_4	-.13	.02	.63*	1.00			
IMPCUSU – Y_5	-.15*	-.06	.57*	.82*	1.00		
IMPCCol – Y_6	-.24*	.17*	.48*	.63*	.56*	1.00	
ODTotT – Y_7	.04	-.22*	-.07	-.01	-.01	-.27*	1.00

Note. *Pearson correlation significant at the .01 level (2-tailed). OWDSenT –Willingness to Disclose Online (Y_1); LevPrivC – Level of Privacy Concern (Y_2) ; IMPCErr – Information Management Privacy Concerns/error (Y_3) ; IMPCIA – Information Management Privacy Concerns/improper access (Y_4); IMPCUSU – Information Management Privacy Concerns/unauthorized secondary use (Y_5); IMPCCol – Information Management Privacy Concerns/collection (Y_6) ; ODTotT – Reported Online disclosure (Y_7).

Inter-item correlations indicated both convergent and discriminant validity with respect to several of the observed variables related to Online Privacy Orientation. Discriminant validity was demonstrated in the relationship between Online Willingness to Disclose (Y_1) and Reported Online Disclosure (Y_7). This finding speaks to the notion that a willingness to disclose seems to have little correlational relationship to reported online disclosure. The findings indicate that a willingness to share personal information does not necessarily engender actual sharing.

A number of other correlations provide additional insight. Online Willingness to Disclose (Y_1) is not correlated with Reported Online Disclosure (Y_7), implying that the information individuals say they are willing to share online does not correspond to actual disclosures during their last online session in which they were asked to share personal information. Researchers have noted a disconnect between individuals' statements

regarding inhibitions related to online activity because of privacy concerns, and their actual levels of online activity. This finding would appear to support those observations.

Further examination of the correlations reveals additional commonalities and disconnects between disclosive intent and activity, and privacy concerns. Information Management Privacy Concerns/collection (Y_6), is the strongest common inhibitor to both Online Willingness to Disclose (Y_1) and Reported Online Disclosure (Y_7). The more general measure of a level of privacy concern, Level of Privacy Concern (Y_2), and Information Management Privacy Concerns/collection (Y_6) share common significant correlations with both Online Willingness to Disclose (Y_1) and Reported Online Disclosure (Y_7). At the same time, Online Willingness to Disclose (Y_1) indicates significant correlations with Information Management Privacy Concerns/error (Y_3) and Information Management Privacy Concerns/unauthorized secondary use (Y_5) whereas Level of Privacy Concern (Y_2) does not.

These findings point to a commonality between Online Willingness to Disclose (Y_1) and Reported Online Disclosure (Y_7), but at the same time reflect heightened concerns with respect to Online Willingness to Disclose (Y_1). This again highlights a disconnect between online disclosive intent and actual online disclosive activity. When individuals are thinking about disclosing personal information online more issues are considered than when they are actually engaged in online disclosive activity.

Online Privacy Orientation consisted of four previously tested and validated indicators addressing Information Management Privacy Concerns and three new untested indicators. Willingness to Disclose Online and Reported Online Disclosure were developed for the study, and Level of Privacy Concern was based on Westin's

work (Harris Interactive, 2002). Level of Privacy Concern, a measure intended to indicate a more general level of concern about information privacy than Information Management Privacy Concerns, along with both Willingness to Disclose Online and Reported Online Disclosure indicated a high large measurement error that may be a function of the fact that both instruments used dichotomous scales. This may have contributed to difficulties in assessing responses. Unlike the Likert-type scales incorporated in the majority of instruments used in the study, dichotomous scales by their nature do not have the level of sensitivity to facilitate response differentiation which may have contributed significantly to the large measurement error evident in the results of these two instruments.

Another potential problem contributing to the large measurement errors for Reported Online Disclosure and Level of Privacy Concern was the number of items retained as a result of data reduction techniques incorporating corrected item-total correlations and factor analysis. Reported Online Disclosure had only three remaining items out of the original 12, while Level of Privacy Concern had only four remaining items of the original seven. Reported Online Disclosure had marginally acceptable reliability ($\alpha = .665$). These factors, all of which impacted results, came under consideration when the final structural model was assessed and are discussed further in connection with modifications made to the structural model.

Consideration of the preceding points related to reliabilities and validity with respect to several of the indicator variables, along with concerns related to sampling brings into question the reliability and validity of the Online Privacy Orientation model. Recognizing the problems with the model does not prevent the results from providing

some insight into the interpretation of its meaning. Online Privacy Orientation reflects individuals' privacy perspective with respect to online disclosure of personal information. Constitutively, Online Privacy Orientation is indicative of the interaction between individuals' willingness to provide personal information online and their concerns about management of online information before or after providing the information.

It is important to remember that Online Privacy Orientation represents a latent construct that is but one aspect of an internalized overall privacy management scheme of an individual that is influenced by Functional Privacy Orientation, as indicated in the structural model. The discussion so far provides proposed definitions for Functional Privacy Orientation and Online Privacy Orientation, addresses problems that may affect their interpretation, and explains the reasoning that led to the final measurement models. This relationship between the two constructs in the structural model will now be discussed.

The Structural Model

The structural model quantitatively describes the relationship between the two latent constructs, Functional Privacy Orientation and Online Privacy Orientation, in terms of the sample data fitting the hypothesized model. The structural model with the loading and disturbance term depicted in Figure 10 is an operationalization of the influence individuals' Functional Privacy Orientation has over their Online Privacy Orientation.

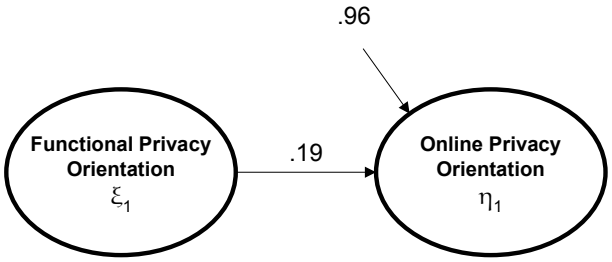
The structural model addresses Research Question 3:

Does Functional Privacy Orientation predict Online Privacy Orientation?

The structural model also addresses the hypothesis:

H_4: Online Privacy Orientation is significantly influenced by Functional Privacy Orientation.

Figure 10. Loading and error estimate of the structural model showing the influence of Functional Privacy Orientation over Online Privacy Orientation.



Both the hypothesis and the research question were supported but must be further qualified. Functional Privacy Orientation exerts a statistically significant influence ($p < .05$) over Online Privacy Orientation but is not a strong predictor of Online Privacy Orientation. Variance extracted was .04, with a residual or unique variance of .96. Holistically, this indicates that Online Privacy Orientation is the product not only of information related concerns and behavior shown in the measurement model, but is also the product of behavior associated with a world view that significantly influences privacy-related behavior as measured by Functional Privacy Orientation. The unique variance of .96 associated with the dependent latent variable Online Privacy Orientation, and a Goodness of Fit Index of .98, indicating that 98% of the variance in the model was explained, make it obvious statistically that this relationship is significantly influenced by other factors absent from the model. Influencing factors not accounted for may be related to the model specification or may be influenced by problems that relate to this specific study, such as the sampling frame. The large unique

variance may also be indicative of significant measurement difficulties associated with several of the indicator variables. Reported Online Disclosure and Willingness to Disclose Online exhibited significant unique variance and could provide fertile ground for further research. A body of literature speaks to the influence of the individual balancing the risks and benefits associated with online behavior.

The measurement models for Functional Privacy Orientation and Online Privacy Orientation explore individuals' personality traits, attitudes, and behavior related to the concept of privacy. Functional Privacy Orientation provides insight into privacy-related behavior in a general way by examining privacy-related behavioral traits. Online Privacy Orientation offers the opportunity to measure individuals' privacy-related behavior and concerns about disclosing personal information in online environments. Holistically these two models provide researchers with new tools that allow them to study the interactions of the related traits and behaviors.

The findings of this study empirically demonstrate a different view of the multidimensionality of privacy and contribute to an understanding of the complexity of the concept, further negating the possibility of a unified coherent definition for the term privacy. The findings also point to reasons for difficulties in attempting to interpret and explain privacy-related behavior. Definitions offered to explain privacy make it difficult to address privacy behavior related issues. The shortcomings of attempts to define or understand privacy are further substantiated by the findings of this study. As a multidimensional concept, privacy challenges any cohesive one-dimensional approach to understanding privacy-related behavior or to addressing the privacy-related concerns of individuals. Anecdotal evidence also provides support for the futility of attempting to

define privacy. What one individual considers private another does not, and this confusion contributes to the difficulties of attempting to interpret privacy-related behavior. The implication for interpreting privacy-related behavior is clear. As Post (1989) says, the researcher interested in privacy should focus on normative behavior.

Methodological Limitations

This study was aggressively designed by virtue of incorporating a large volume of material. The goals were to explore various behavioral traits commonly linked to privacy and to develop new approaches for studying online privacy-related behavior. These goals could not be met using a short simple instrument. The complexity of the instrument was necessary in order to address the research questions and hypotheses. These ambitious goals presented challenges with the length of the survey instrument, which was composed mostly of instruments used in previous studies. In this study, reliabilities of many of the existing instruments were either below or at the low end of the results reported in earlier studies. The study sample was demographically restricted, potentially compromising external validity. These limitations are reviewed along with their impact on the reliability and subsequent interpretability of the findings.

Sampling

As previously discussed, analysis of covariance structures is a statistical method intended for large samples. In an attempt to address this requirement, 700 surveys were distributed to volunteers at various locations. Completed surveys amounted to a response rate of 24%. Although 105 contained missing responses, data imputation resulted in 274 usable surveys. This sample size is considered small but adequate for the analysis of relatively simple covariance structures.

While an attempt was made to seek diversity in the sample composition, this objective was not reached. Most of the respondents consisted of white females with some college-level experience. There were also indications that the participants' limited education contributed to some difficulties understanding the statements and questions being presented. Some participants indicated that they had to "look up" various terms used in the survey before they could respond.

While the primary targeted participant pool consisted of the faculty, staff, and students of a community college, there was minimal participation by faculty and staff. Only 17 of a potential 200 faculty and staff chose to fill out the survey. The sampling technique was also intended to draw on a larger group of older adults typically found in night classes. This too did not turn out to be the case. This marginal participation by older, better educated, more experienced adults contributed to the fact that only 64 of 274 respondents had a college degree.

Another problem lies with the age of the respondents. The mode for age was 20, and 34% of the sample was under the age of 25, indicating the sample was skewed with respect to age. The combination of the tightly grouped demographics and lower level of education has the potential to impact results, thus diminishing external validity. It can be concluded that participants' education level and limited life experiences contributed to difficulties in their ability to understand what was being asked or to comprehend the substance of the statements they were presented. This type of problem can be addressed only through sampling procedures that reach a more representative audience of participants, which was obviously not the case with this study.

Reliability and Validity

A potential threat to internal validity is evidenced based on the reliability of the observed variables used in the study. As discussed in chapter 4, several of the measurements, particularly Locus of Control/internal, indicated low internal consistency. The reported reliability for each instrument was consistent with prior findings but still raises a question about the reliability of the measures and the resulting impact on the measurement models and the structural model. The scope of the study provided for an assessment of related constructs, and it is noted in chapter 4 and previously in this chapter that there were significant indications of both convergent and discriminant validity.

Survey Instrument Design

The length of the survey appears to have precipitated a number of problems. It probably contributed to a reduction of the number of participants and the degree of completion by those who chose to participate. The 700 surveys distributed were given only to those who had agreed to participate. A 24% completion rate would be considered a good response rate in a randomly distributed anonymous survey, particularly a survey instrument of this length. In the case of a volunteer participant base, this response rate may be indicative of problems with the survey instrument, the sampling frame, or both. Skipped pages in the returned surveys might indicate haste or frustration on the part of the participant because of the length of time required to complete the instrument, or as mentioned above, the inability of the participant to comprehend the material. The missing responses might also indicate frustration based on an inability to relate to what was being asked because as a function of youth or

general life experiences. This observation, combined with the fact that 61% of the volunteers did not even return the survey, raises questions about the design of the instrument. The length might not have been the only intervening factor in the response rate. Other factors such as the nature of the material, which some would consider sensitive, or the inability to understand some of the material may also have contributed to the low response rate.

Implications of Results

The focus of this study was an exploration of the relationships between behavioral traits, privacy concerns, and online information behavior. In prior research many of the relationships were studied as binary interactions, that is, the relationship of one construct to another individual construct such as trust and self-disclosure (Wheeless & Grotz, 1977); privacy and online behavior (Annacker, Spiekermann, & Strobel, 2001); disclosure and online behavior (Phelps, Nowak, & Ferrell, 2000; White, 1999); and risk and trust (Das & Teng, 2004). Privacy has been the focus of marketing research as a function of targeted advertising, and consequences of a perceived invasion of privacy (Phelps, Souza, & Nowak, 2001). Concerns about the collection, use, aggregation, and dissemination of personal information have also been debated and studied, spurred by the pervasive and invasive nature of the technological environment that began to evolve after World War II (Barber & Lanz, 2000; Culnan & Milberg, 1999; Garfinkel, 2000; Westin, 1967). This significant amount of prior research laid the foundation for the theoretical and methodological approach used in this study.

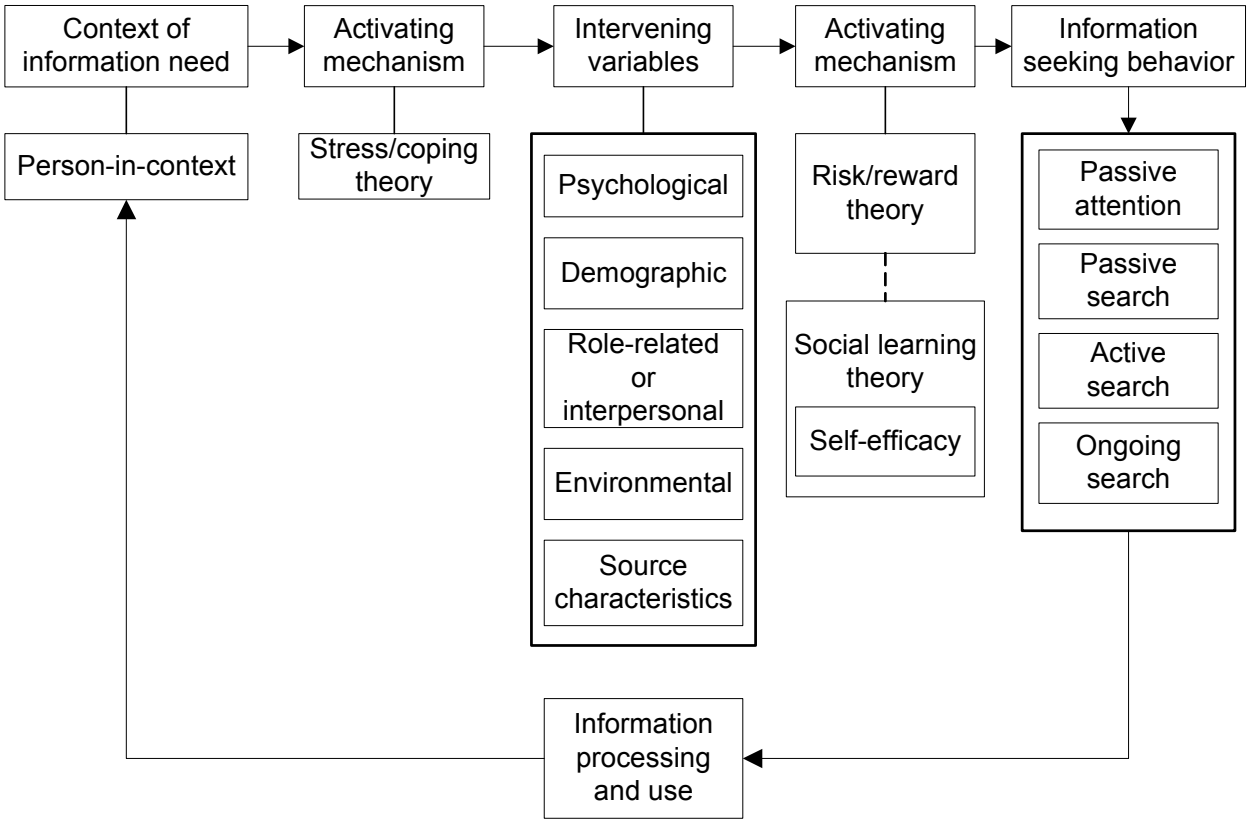
Theoretical concept of privacy

Through various avenues of research mentioned previously, investigators have been able to identify and define many privacy-related personality traits such as disclosure, sense of control, trust, and risk. Even though these concepts have been linked to the concept of privacy in prior research, there is an apparent lack of theoretical understanding about the interaction of these factors, their interaction and relationship to privacy, and consequent information behavior. This study brings into focus the relationships of several of these privacy-related constructs and their influence not only on individuals' underlying attitudes and privacy-related behavior, but also more generally on the relationship of these various constructs to information behavior.

Wilson's 1996 model of information behavior depicted in Figure 11 provides a relevant framework. The scope of this study speaks to two primary areas in his model. The first area is intervening variables. Wilson (1999) points out ". . . the use of the term 'intervening variables' serves to suggest that their impact may be supportive of information use as well as preventive . . . " (p. 256). Wilson's notion of intervening variables addresses the complex nature of the psychological impact on an individual's privacy posture and associated information behavior. This study is inclusive of both the social psychological and individual psychological spheres of interest within Wilson's framework. Individuals involved in a dynamic process of deciding to share information about themselves have simultaneous and opposing influences shaping their decisions. These opposing influences are quantitatively operationalized through Functional Privacy Orientation and are revealed in the bipolar nature of the construct. This same type of conflict is depicted in Online Privacy Orientation, that of balancing disclosure of

personal information while simultaneously balancing concerns about the manner the information will be handled once it has been released. The influence of Functional Privacy Orientation on Online Privacy Orientation quantitatively depicts a further behavioral and cognitive process, that is, a dynamic balancing all of the influences before deciding to provide or withhold personal information.

Figure 11. Wilson's 1996 model of information behavior.



Note. Copyright 1996 by T. D. Wilson. Reprinted with permission.

A second relevant area in Wilson's model is risk/reward theory, shown as an activating mechanism influencing information behavior. As Petronio (2002) aptly states, "One reason we find it necessary to control our privacy boundaries is because we need to balance the risks and gains of revealing private information." (p. 65). Once again, this

study provides a holistic quantitative representation of the interaction and relationships of these competing and influential mechanisms.

Functional Privacy Orientation is an amalgam of conflicting social and psychological influences that determine the manner and degree of people's openness in society. It is evident from the relationships in the model that a reduced sense of control over privacy, that is, a drop in Functional Privacy Orientation, influences a number of factors such as the information people choose to share, a perception of vulnerability to the influence of powerful others or chance, and a sense of risk taking. Conversely, a rise in Functional Privacy Orientation positively influences the honesty and accuracy of disclosures, one's sense of control over our life events, and general trust.

The key contribution of this evaluation is the degree to which various quantifiable factors are influenced by a need for privacy-oriented behavior. Petronio's idea of information control is neither new nor unique. The idea of Big Brother is pervasive in the literature surrounding privacy. In an analogy employing Kafka's *The Trial*, Solove (2002) makes a cogent point by discussing the perceived loss of control and resulting vulnerability people feel with respect to the collection and dissemination of their personal information. Returning to Wilson's intervening variables, the notion of loss of control over personal information likely becomes a psychological impediment to information sharing. This study provides a mechanism in the form of Functional Privacy Orientation by which to recognize the nature of the interactions that lead to this potential impediment.

Methodological Implications

Two new instruments for measuring online disclosive behavior were developed for this study. The new instruments provide an innovative framework for researchers to study privacy. Structural equation modeling was used to assess the relationships of the eight instruments used to measure attitudes and behavior related to privacy. Structural equation modeling provided the framework for a holistic assessment of privacy behavior and attitudes. From a methodological perspective the approach incorporated into, and findings of this study demonstrate the capacity to quantitatively and simultaneously examine the interactions of proposed indicator variables and affective latent constructs.

The two new instruments, Online Willingness to Disclose and Reported Online Disclosure, were designed to measure a willingness to disclose personal information online, and actual online disclosive behavior. Online Willingness to Disclose provides insight into the attitudes of individuals about online disclosure, an assessment of what they think they would do in a given online situation that requests personal information. Reported Online Disclosure is designed to measure actual online disclosiveness during online activities that request personal information. Given similar online situations this approach provides a view of the disconnect between what people say they would do and what they actually do when providing personal information online. Based on the results of the study this approach is promising, but refinement of the instruments is needed.

Westin (1967) scrutinized privacy in relation to control over personal information. His approach of using opinion polls to gauge public posture with respect to information control established a framework for speaking about privacy perception in terms of

information control. However, his approach by virtue of its very purpose never investigated its relationship at the level of the individual. In this study, using structural equation modeling and personality traits such as General Disclosiveness, Locus of Control, Generalized Trust, Risk Orientation, and Risk Propensity an individual's inherent concept of control is linked to the responses related to online privacy behavior. The results indicated that these personality traits, used as indicators of Functional Privacy Orientation, significantly influence online behavior and privacy concerns related to Online Privacy Orientation.

The same approach, using indicator variables to measure latent constructs, is a viable approach for quantitative assessment of Petronio's (2002) model. Researchers incorporating various indicators to study the influence of the boundary construct on theorized indicator variables could refine the definition of privacy boundaries, furthering the understanding of interactions that influence their establishment and maintenance.

Wilson's (2000) comprehensive model of information behavior also lends itself to this type of holistic modeling of indicator variables and latent constructs. Many of the contributing factors, such as the psychological constructs this study addressed, are latent constructs. Structural equation modeling could contribute to a better understanding of the interactions between the various formative indicators and latent constructs delineated in his model.

Functional Implications

It is commonly acknowledged that the concept of privacy is difficult if not impossible to define because of its subjective nature and susceptibility to psychological and contextual influences. The notion that it can be substantively addressed as a

concept in its own right is misguided. Researchers who address the concept of privacy without a succinct definition gather data based on a concept that is actually conceived by the subjects of the investigation. Because the researchers are unaware of the individual's subjective interpretation of privacy, the results of their research are ambiguous and possibly misleading.

Public and private organizations seeking to understand privacy in order to formulate policy should begin by understanding that privacy cannot be measured directly in the context of an opinion survey. Opinion surveys speak to the mental state of individuals at a point in time. Privacy must be addressed both in terms of an individual's Functional Privacy Orientation and the specific domain of interest, whether it be an online environment, access to or use of medical or financial records, political or religious views, or any other area of concern. This study, and holistic frameworks such as Wilson's provide alternative avenues for investigation.

Future Research

One goal of this research effort was an attempt to quantify and examine the relationships between personality traits commonly associated with privacy, concerns related to privacy and management of personal information, and online information behavior. This study attempted to clarify the messages that individuals, both as consumers and providers of information, provide in various studies and polls dealing with the concept and issues surrounding privacy.

There has always been an inconsistency between what users say they do online and what they actually do in online environments. The methods associated with assessing online behavior; measuring concerns through opinion surveys, measuring

activity in artificial environments, or detailed self-reports of online activity, present a number of challenges in attempting to understand the associated realities. Recognizing these difficulties, researchers need to address online activity using a multifaceted approach similar to the approach used in this study.

Two instruments developed for this study provide a basis for new directions in evaluating individuals' attitudes related to online behavior. The first instrument, Willingness to Disclose Online, attempted to evaluate an intent or attitude related to online disclosure, providing a mechanism to differentiate an inclination to disclose from actual online disclosure. A perceived willingness on the part of the individual to disclose information online offers additional insight into the attitudes related to online behavior and privacy and provides an additional dimension for measuring online perceptions, fears, and concerns related to the management of personal information. The base instrument with 59 items provided some basic insights. Almost all respondents were willing to provide certain types of fundamental information about themselves. Responses also indicated certain items with high variability or inconsistency, such as religious and political affiliations that present opportunities for further discrimination of fundamental attitudes. Other items, those used in the final analysis, provided insight into the types of information individuals consider sensitive, but given reasonable circumstances or adequate benefits, might be willing to provide. These items, which were measured as a dichotomy, form a basis for investigating a willingness to disclose certain types of information, or insight into a potential area of sensitivity differentiation. Development of a scaled instrument, capable of providing a reliable and valid measure of this phenomenon, should provide a base perspective for more effectively measuring

the difference between what individuals indicate they are willing to share online and what they actually do online. The differential between what individuals say and actually do in online environments has been studied but to date has not been effectively addressed. This conflict was reflected in the results of this study. The question of intent with respect to online behavior requires investigative techniques that are less intrusive, less mentally taxing, and less subject to the influences of recall and artificial environments.

The second instrument, a simple evaluation of a prior online experience, can provide a basis for comparison between individuals' expressed intent and their actual activities. Prior research that attempted to gauge actual online behavior depended heavily on either activity log analysis, which is data rich and information sparse; detailed self-reports which are subject to the error associated with accurate recall; or the establishment of artificial environments to study online behavior, a method subject to the influence of the research environment. Further work along the line of investigation pursued in this study should prove both productive and informative. The question remaining is whether or not there are more effective means of measuring actual online activity.

The second major area that was investigated in this study was the relationship between states and traits, states being more temporally fluid than traits (Nunnally & Bernstein, 1994). Individual behavioral characteristics that appear to be temporally stable, such as locus of control, trust, and risk, were assessed in relation to online behavior and concerns. Social science research, by its nature, examines individuals' interpretations of, reactions to, and behavior in a given social environment. Information

behavior research addressing online behavior should embrace this approach by focusing more on individuals' stable traits, depending less on reactionary responses to opinion-based surveys. Researchers need to develop a basic set of temporally stable criteria for assessing individuals' privacy concerns and online behavior.

Opinion polls offer government and business alike a snapshot of subjects' response to a situation at a particular time, place, and in a unique mental state. Research needs to be developed that provides a more temporally stable network of base evaluative criteria on which to assess response and reaction to privacy-related issues. Opinion polls are snapshots of individuals' interpretation of and reaction to social and cultural environments. As such, the decision making processes that use opinion polls for anything more than feedback mechanisms are basing decisions on reactionary responses and environmental issues that may ultimately result in poor solutions. This results in short-term benefits but unknown long-term impacts. Opinion polls that deal with privacy issues, such as those conducted by Harris, should be used as gauges and not guidelines for policy makers in formulating long-term approaches in both business and government organizations. They should also be used to gauge reaction to the impact of technology and not be used to establish direction.

Research such as this can facilitate technology planning and policy formulation. Opinion polls fail to reveal more substantial underlying bases for behavioral response. While the use of opinion polls may address currently perceived needs, the proper course of action may not be apparent until potentially damaging and costly practices and policies have been adopted. This will only lead to further issues and problems requiring additional fixes or to more complex solutions that require more resources than

would have been needed initially had a better understanding of the behavior been developed.

Summary

This research provides a foundation for a new approach to understanding the multidimensional concept of privacy. It is relevant to government agencies concerned with privacy that examine and establish practice and policy, business or other organizations attempting to interpret the privacy concerns of their clients, or individuals trying to communicate concerns about privacy.

From another perspective, this study has established an approach and framework that relates the behavioral aspects of individuals as they exist in society and culture, aspects that establish attitudes resulting in the individual's normative realization of privacy. No attempt was made to define privacy, recognizing that past attempts to do so by even those most knowledgeable have fallen short. Many facets of this study present a common thread in attempting to examine normative behavior associated with privacy, that common thread being vulnerability. Vulnerability comes in the form of the risk associated with trusting another or revealing oneself, or the loss of control over information that defines a person in a social context, shaping the perceptions of others about that person.

For public and private organizations, as well as individuals, privacy contributes to accomplishing goals, enhancing competitiveness, and contributing to survival in an online and connected world. So the common thread of vulnerability extends to all cultures and all levels of social activity and requires that all participants recognize and respect the vulnerabilities that a lack of privacy in any venue may create for all. As

discussed in chapter 2, any organization has difficulty managing its affairs when scrutinized under the glaring light of full disclosure. Conversely, organizations must also recognize that the difficulties they experience as a consequence of unintended disclosures that impact their activities and actionable options are also experienced by individuals they choose to scrutinize.

This study sought to evaluate the interrelationships of personality characteristics commonly associated with privacy and the sharing of personal information in conjunction with behaviors and the perceptions and concerns individuals espouse with respect to online information environments. The approach used for this effort appeared self-evident in that research cannot evaluate information behavior outside the context of an individual's perceptual and behavioral social reality. Any attempt to isolate particular behaviors or perceptions outside the context of their influencing factors will provide results that at the least are difficult to interpret, and at the worst provide direction for decisions or further research devoid of substantive foundations.

When reviewed in the context of the current social and political environment, this study provides guidance for a holistic interpretation of information behavior with respect to privacy in online environments. It was conceptualized in part by the recognition that opinion polls provide an overview of the environment that they seek to analyze at a given point in time, and the fact that this was providing an inappropriate basis for both policy and technology direction. Opinion polls should not provide direction for long-term policy decisions or technology direction, whether it be a public or private organization.

Functional Privacy Orientation was defined in the context of this study as an indicator of an individual's privacy-oriented behavior with respect to perceived control of

personal information in a general context. Online Privacy Orientation was defined in the context of this study as an indicator of an individual's underlying privacy-related behavior related to sharing information in online environments. This holistic approach not only better addresses the interaction of the behavioral traits that relate to the individual sharing information, but also relates these traits to information behavior in an online environment.

The use of opinion polls to measure privacy attitudes, whether in online or offline environments, reveals only half the picture. To effectively address privacy concerns and the resulting behavioral fallout in an online environment research must also address the social, personal and cultural influences that shape the individual's privacy-related attitudes with respect to the area being investigated. Future research must address and differentiate various triggers that influence the behaviors and attitudes they are trying to understand.

APPENDIX A

FINAL SURVEY INSTRUMENT

Table 16 indicates locations, modifications, and sources of the various instruments incorporated in the final survey instrument.

Table 16
Privacy Disposition Inventory Sub-instruments: Location in Survey and Items

Construct Measured	Begins Page	Total Items Utilized(original)	Notes
General Disclosiveness [1]	158	20 (31)	
Locus of Control [2]	160	24 (24)	
Generalized Trust [3]	162	15 (13)	
Risk Orientation [4]	156	12 (14)	2 items added
Risk Propensity [4]	157	5(5)	
Willingness to Disclose Online	166	59 (n/a)	new instrument
Level of Privacy Concern	165	9 (3)	6 items added
Information Management Privacy Concerns [5]	164	15 (15)	scale reversed
Reported Online disclosure	163	13 (n/a)	new instrument

Notes. [1] Copyright 1978 by Lawrence R. Wheeless. Adapted with permission. [2] Copyright 1981 Elsevier. Adapted with permission. [3] Copyright 1977 by the International Communication Association. Adapted with permission. [4]Copyright 2002 by Bernd Rohrmann. Adapted with permission. [5] Copyright 1996 by the Management Information Systems Research Center (MISRC) of the University of Minnesota and the Society for Information Management (SIM). Adapted with permission.

Privacy & Personal Information: A Survey

This survey is intended to explore some of the ways people feel about themselves and other people, and how they relate to the world around them. It is administered anonymously in the hope that those willing to participate will feel comfortable responding to all of the items without concern for things that might otherwise make them uncomfortable, such as sharing personal information with someone they don't know. Please make sure you do not sign your name or place any other kind of identifying mark on the survey. The survey should take around 25 minutes to complete.

There are no right or wrong answers. Answers can only be compared to the answers of others that have completed this survey or one similar. Replies cannot be compared to any type of index or scale that would indicate anything more, such as would be the case with something like an IQ test.

Please don't try to second-guess yourself. Generally the first response that you give is the closest to how you actually feel about something, and how you feel is what this is all about.

Different methods or scales are used on the survey to indicate your views, perspectives, or feelings about the statements. There are specific instructions for various portions of the survey. There are some general questions about you at the end of the survey. I appreciate your willingness to share your feelings, your candidness, and your honesty. If you have any questions please feel free to ask. You may contact me as indicated on the Research Project Information Sheet that was included in your survey package.

Thank you very much.

Brian Grams

Instructions: Read each statement carefully. Circle the number on the scale that is the closest description of the way you feel about the statement. First impressions are usually best. Please be sure to respond to every statement. If the numbers used for answers do not adequately reflect your own opinion, use the one that is closest to the way you feel.

1. I'm very careful when I make plans and when I act on them.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
2. I follow the motto, 'nothing ventured, nothing gained'	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
3. I don't have much sympathy for daring decisions.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
4. Quite often I will do things I haven't done before without seriously thinking about it.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
5. If a task seems interesting I'll choose to do it even if I'm not sure whether I'll be able to manage it.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
6. I don't like to risk things; I would rather be on the safe side.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
7. Even when I know that my chances of success are limited, I will try my luck.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
8. In my work I set goals so that I can achieve them without difficulty.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
9. I express my opinion even if most people have opposite views.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
10. My decisions are always made carefully and accurately.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
11. I would like my boss's job some time so I could show my competence, despite the risk of making mistakes.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
12. I tend to think about the unfavorable outcomes of my actions.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
13. Success encourages me to take bigger risks.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
14. If I really want to do something, I will go ahead, do it, and worry about the consequences later.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me

Some activities involve a "*physical*" risk, such as particular occupations (e.g. fireman, policeman, military) or sports (e.g. rock-climbing, skydiving) or transportation (e.g. cycling) - that is, there is a risk of getting injured in an accident or possibly even being killed. 15. In general, my tendency to accept ***physical*** risks is...	**1** Extremely Low **2 3 4 5 6 7 8 9 10** Extremely High
Some activities involve a "financial" risk, such as starting a business, investing in the stock market, or gambling (e.g. in casinos) and betting (e.g. on horses) - that is, there is a risk of losing money or other assets. 16. In general, my tendency to accept ***financial*** risks is ...	**1** Extremely Low **2 3 4 5 6 7 8 9 10** Extremely High
Some activities involve a "health" risk, such as traveling overseas (e.g. in countries of low hygienic standards) or particular "lifestyle" behaviors (e.g. long sunbathing, unsafe sex, drugs for pleasure) or smoking - that is, there is a risk of catching a harmful disease. 17. In general, my tendency to accept ***health*** risks is ...	**1** Extremely Low **2 3 4 5 6 7 8 9 10** Extremely High
Some activities involve a "*social*" risk, such as being outspoken or behaving in an unusual manner (e.g. openly challenging or disagreeing with commonly accepted views, deviating sexually, or violating social norms) or accepting public roles (e.g. giving an unpopular or controversial speech) - that is, there is a risk of losing the respect and acceptance of others and harming one's social status. 18. In general, my tendency to accept ***social*** risks is ...	**1** Extremely Low **2 3 4 5 6 7 8 9 10** Extremely High
19. Overall, how would you rate your general willingness to take a risk *in comparison to other people*, such as your family, friends, or acquaintances?	**1** Extremely Low **2 3 4 5 6 7 8 9 10** Extremely High

Instructions: Please mark the following statements to reflect how you communicate with people in general. Indicate the degree to which the following statements reflect how you communicate with people by circling the number on the scale that is the closest to a description of the way you feel about the statement. Please be sure to mark all statements.

1. I do not always feel completely sincere when I reveal my own feelings, emotions, behaviors or experiences.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
2. I intimately disclose who I really am, openly and fully in my conversation.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
3. I do not often talk about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
4. Only infrequently do I express my personal beliefs and opinions.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
5. I am not always honest in my self-disclosures.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
6. Once I get started, my self-disclosures last a long time.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
7. I often talk about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
8. I always feel completely sincere when I reveal my own feelings and experiences.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
9. I feel that I sometimes do *not* control my self-disclosure of personal or intimate things I tell about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
10. I am often not confident that my expressions of my own feelings, emotions, and experiences are true reflections of myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
11. My conversation lasts the least time when I am discussing myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree

12. My statements about my feelings, emotions, and experiences are always accurate self-perceptions.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
13. I often disclose intimate, personal things about myself without hesitation.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
14. I often discuss my feelings about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
15. Once I get started, I intimately and fully reveal myself in my self-disclosures.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
16. My self-disclosures are completely accurate reflections of who I really am.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
17. I usually talk about myself for fairly long periods at a time.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
18. I cannot reveal myself when I want to because I do not know myself thoroughly enough.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
19. My statements of my feelings are usually brief.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
20. I am always honest in my self-disclosures.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree

Instructions: The following 24 items are a series of attitude statements. Each represents a commonly held opinion. There are no right or wrong answers. You will probably agree with some items and disagree with others. We are interested in the extent to which you agree or disagree with such matters of opinion.
Read each statement carefully. Then indicate the extent to which you agree or disagree by circling the number on the scale that is the closest description of the way you feel about the statement. First impressions are usually best. Please be sure to respond to every statement. If you find that the numbers used in answering do not adequately reflect your own opinion, use the one that is closest to the way you feel.

	-3	-2	-1	1	2	3
1. Whether or not I get to be a leader depends mostly on my ability.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
2. To a great extent my life is controlled by accidental happenings.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
3. I feel like what happens in my life is mostly determined by powerful people.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
4. Whether or not I get into a car accident depends mostly on how good a driver I am.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
5. When I make plans, I am almost certain to make them work.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
6. Often there is no chance of protecting my personal interests from bad luck happenings.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
7. When I get what I want, it's usually because I'm lucky.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
8. Although I might have good ability, I will not be given leadership responsibility without appealing to those in positions of power.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
9. How many friends I have depends on how nice a person I am.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
10. I have often found that what is going to happen will happen.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree

	-3	-2	-1	1	2	3
11. My life is chiefly controlled by powerful others.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
12. Whether or not I get into a car accident is mostly a matter of luck.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
13. People like myself have very little chance of protecting our personal interests when they conflict with those of strong pressure groups	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
14. It's not always wise for me to plan too far ahead because many things turn out to be a matter of good or bad fortune.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
15. Getting what I want requires pleasing those people above me.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
16. Whether or not I get to be a leader depends on whether I'm lucky enough to be in the right place at the right time.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
17. If important people were to decide they didn't like me, I probably wouldn't make many friends.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
18. I can pretty much determine what will happen in my life.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
19. I am usually able to protect my personal interests.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
20. Whether or not I get into a car accident depends mostly on the other driver.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
21. When I get what I want, it's usually because I worked hard for it.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
22. In order to have my plans work, I make sure that they fit in with the desires of people who have power over me.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree

	-3	-2	-1	1	2	3
23. My life is determined by my own actions.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
24. It's chiefly a matter of fate whether or not I have a few friends or many friends.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree

Instructions: On the scales that follow, please indicate your reaction to people in general. Place a check ✓ in the box that represents your immediate feelings about people. Check in the direction of the end of the scale that seems to be the most characteristic of the people you deal with on a daily basis. Place only one check on each line and please mark all lines.

I feel that most people are:

Trustworthy	☐	☐	☐	☐	☐	☐	☐ Untrustworthy
Exploitive	☐	☐	☐	☐	☐	☐	☐ Benevolent
Secretive	☐	☐	☐	☐	☐	☐	☐ Talkative
Safe	☐	☐	☐	☐	☐	☐	☐ Dangerous
Deceptive	☐	☐	☐	☐	☐	☐	☐ Candid
Not deceitful	☐	☐	☐	☐	☐	☐	☐ Deceitful
Tricky	☐	☐	☐	☐	☐	☐	☐ Straightforward
Respectful	☐	☐	☐	☐	☐	☐	☐ Disrespectful
Inconsiderate	☐	☐	☐	☐	☐	☐	☐ Considerate
Honest	☐	☐	☐	☐	☐	☐	☐ Dishonest
Unreliable	☐	☐	☐	☐	☐	☐	☐ Reliable
Insincere	☐	☐	☐	☐	☐	☐	☐ Sincere
Careful	☐	☐	☐	☐	☐	☐	☐ Careless
Confidential	☐	☐	☐	☐	☐	☐	☐ Divulging

1. ☐ **Mark this box if you have *never* provided information to a Web site online then move on to the next section.**

Instructions: Think about the last time you volunteered to give a Web site information about yourself to get something in return, such as providing personal information for a purchase or to acquire some other type of benefit from the site. You may or may not have identified yourself, but still provided personal information. Based on your memory of that experience are the following statements about various aspects or impressions of your online experience true (T) or false (F)? Place a check ✓ in the appropriate box.

2. ☐ T ☐ F The Web site can tell exactly who I am with the information I provided.

3. ☐ T ☐ F The Web site requested too much personal information for what it was offering in return.

4. ☐ T ☐ F I can't control what will be done with information I provided at the Web site.

5. ☐ T ☐ F I provided only required information to get what I wanted and skipped the rest.

6. ☐ T ☐ F The Web site requested too much personal information, so I left without finishing.

7. ☐ T ☐ F Some of the personal information requested made me uncomfortable, but I provided the information anyway.

8. ☐ T ☐ F I provided information that I wouldn't want to give to just anyone.

9. ☐ T ☐ F I checked the Web site to see what would be done with my information before I provided it.

10. ☐ T ☐ F All the information I did provide was accurate and honest.

11. ☐ T ☐ F I didn't provide all the information that was requested.

12. ☐ T ☐ F I checked to see if the site was secure before I provided any information

13. ☐ T ☐ F I checked the Web site's privacy policy before providing any information.

Instructions: The following statements are intended to relate to your feelings about other people who have access to and use of, or otherwise deal with your personal information. Personal information includes, among other things, information about you that can be used to identify you as an individual such as your name, phone number, address, credit card numbers, and Social Security number. Personal information may also include information about you that you wouldn't want the general public to have access to, or know about and be able to associate with you in particular. This type of information may include knowledge such as specific things that have happened to you, things you have participated in such as political activism, or such things as your personal preferences, habits, or behaviors. Using the scale to the right of each statement, indicate your level of agreement with the statement by circling the number on the scale that is the closest description of the way you feel about the statement.

1.	It usually bothers me when companies ask me for personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
2.	All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
3.	Companies should not use personal information for any purpose unless it has been authorized by the individual who provided the original information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
4.	Companies should devote more time and effort to preventing unauthorized access to personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
5.	When companies ask me for personal information, I sometimes think twice before providing it.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
6.	Companies should take more steps to make sure that the personal information in their files is accurate.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
7.	Government regulation is the best way to protect my personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
8.	When people give personal information to a company for some reason, the company should never use the information for any other reason.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
9.	I am comfortable with the ways most companies use my personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
10.	Companies should have better procedures to correct errors in personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
11.	Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree

12. It bothers me to give personal information to so many companies.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
13. Companies should never sell the personal information in their computer databases to other companies.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
14. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
15. I believe that personal information I have provided online is generally used the way I expected.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
16. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
17. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
18. I'm concerned that companies are collecting too much personal information about me.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
19. Consumers have lost all control over how personal information is collected and used by companies.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
20. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
21. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
22. Being able to control my information is more important than protecting my privacy.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
23. I feel that going online jeopardizes my privacy.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree
24. Too many companies have access to my personal information without my consent.	1 Strongly Agree	2	3	4	5	6	7 Strongly Disagree

Situation: A publisher (sports or health magazine, newspaper, world news, etc.) will provide you with a special free premium online version of its publication containing advice, editorials, late-breaking news, and discounts at some of its advertiser's stores. You think the offer is attractive and would like access to the premium content, which will be made available online even if you don't subscribe to the publisher's print publication. All you have to do is agree to share some requested information about you. The information will be collected at the publisher's online Web site with the condition that all requested information **must** be provided in order to access the premium content.

Instructions: The following is a list of information items a publisher **could** request. You have decided that you really want access to the free premium content being offered. **Place a check** ✓ to indicate each information item **you would be willing to provide** in the appropriate box, **yes (Y), no (N), or does not apply to me (N/A)**. Even if a piece of information seems redundant please indicate your willingness to provide that piece of information.

Contact Information		
[Y] [N] Home mailing address	[Y] [N] [N/A] Your email address	[Y] [N] Zip code
[Y] [N] Your full name	[Y] [N] City of residence	[Y] [N] State of residence
[Y] [N] [N/A] Your cell phone number	[Y] [N] [N/A] Home phone number	[Y] [N] [N/A] Your work phone number
[Y] [N] [N/A] Street address (if you get mail at a P. O. Box)		
Likes/Dislikes		
[Y] [N] Favorite food	[Y] [N] Favorite TV show	[Y] [N] Favorite hobby
[Y] [N] Favorite book	[Y] [N] Favorite recording artist	[Y] [N] Favorite movie
[Y] [N] Favorite periodical (magazine, journal, newspaper, etc.)	[Y] [N] Preferred political party	[Y] [N] Favorite sports team
Spouse's Information (skip this section if you are not currently married.)		
[Y] [N] Spouse's weight	[Y] [N] Spouse's height	[Y] [N] Spouse's birthday
[Y] [N] Number of people in household	[Y] [N] Spouse's date of birth	[Y] [N] Married on what date
Children's Information (skip this section if you do not have school age children living with you.)		
[Y] [N] Number of children	[Y] [N] Children's gender	[Y] [N] Children's ages
[Y] [N] School children attend	[Y] [N] Children's names	
Personal Information		
[Y] [N] Your citizenship	[Y] [N] Own or rent residence	[Y] [N] Your date of birth
[Y] [N] Mother's maiden name	[Y] [N] Your ethnicity	[Y] [N] Marital status
[Y] [N] State you were born in	[Y] [N] Your education (number of years)	[Y] [N] [N/A] Number of credit cards you own
[Y] [N] Religious preference	[Y] [N] [N/A] Value of owned residence	[Y] [N] Your gender

Medical Information

[Y] [N] Personal physician's name	[Y] [N] Your blood type	[Y] [N] [N/A] Your handicaps
[Y] [N] [N/A] Prescribed medications you use	[Y] [N] [N/A] Non-prescription medications you use	[Y] [N] Date of your last illness/injury
[Y] [N] Nature of last illness/injury	[Y] [N] Your weight	[Y] [N] Your height

Identification

[Y] [N] Your driver's license number	[Y] [N] Your social security number	[Y] [N] [N/A] Your employer or student ID number

Employment Information (skip this section if you have never been employed.)

[Y] [N] Your occupation	[Y] [N] Your income	[Y] [N] Your employer
[Y] [N] Household income	[Y] [N] How long in your current job	

Instructions: The following information that we are asking you to provide will help us understand you a little better. Please check the answer that best describes your activities or habits, or provide the appropriate answer in the space provided.

1. ___ I own or have access to a computer

(If you did not check the above statement please skip to question 8)

2. I have been using a computer:
   ___ less than a year
   ___ 1 to 5 years
   ___ over 6 years

3. ___ I use a computer for online access to the Internet/World Wide Web

(If you did not check the above statement please skip to question 8)
(check only one)

4. ___ I use my own computer most of the time for online access

5. ___ I use someone else's computer most of the time for online access (such as those available in a library or school)

6. I have been using a computer to get online:
   ___ less than a year
   ___ 1 to 3 years
   ___ over 3 years

7. I get on the Web to do things other than check email or play interactive games:
   ___ several hours every day
   ___ every day
   ___ a few times a week
   ___ not very often

8. On average I purchase things online:
   ___ every month
   ___ every couple of months
   ___ hardly ever
   ___ never

9. I am a: ___ Female ___ Male

10. I was born in the year: 19 _____

11. I am married: ____ Yes ____ No

12. I take care of _____ dependent children in my home.

13. I live with my family or someone else other than a spouse who provides support.
___ Yes
___ No

14. My ethnicity is:
___ White
___ African-American
___ Hispanic
___ Asian/Pacific Islander
___ American Indian/Alaskan Native
___ Nonresident Alien
___ Mixed
___ Unknown

15. My level of education is: (Please check only the highest level you have completed)
___ High-school diploma or equivalent
___ Licensed or certified skill not requiring a 4 year degree
___ Some college
___ Bachelor's degree
___ Graduate degree

16. My employment status is:
___ Full-time
___ Part-time
___ Not currently employed, not looking for a job
___ Not currently employed, looking for a job

17. My annual income range is:
___ Less than $15,000
___ $15,000 to $25,000
___ $25,000 to $35,000
___ $35,000 - $50,000
___ $50,000 - $75,000
___ $75,000 or more

18. Have you ever had information about you used illegally such as with credit card or checking fraud, or identity theft?
___ Yes
___ No

19. Are you aware if any company has ever used your personal information without your permission in a way you didn't like?
___ Yes
___ No

Please take a moment to check the booklet to be sure you have not skipped any pages, statements or questions.

20. If you would like, make any comments or offer any suggestions you might have about this survey. Continue on the remaining blank pages if you would like to use more space.

APPENDIX B

LISREL OUTPUT FOR MEASUREMENT AND STRUCTURAL MODELS

DATE: 11/15/2004

TIME: 20:13

L I S R E L 8.54

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140

Functional Privacy Orientation – Initial Measurement Model

```
Observed Variables:
Gtrust GSDAmt GSDCon GSDHon LOCIntr LOCPOr LOCChar ROPro
ROCare RiskPro IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC OWDSenT
ODTotT

Correlation Matrix from file FPOFin1115.cor
Asymptotic Covariance matrix from file FPOFin1115.acm

Sample Size = 274
Latent variable: FunPriOr

Relationships:
Gtrust GSDAmt GSDCon GSDHon LOCIntr LOCPOr= FunPriOr
LOCChar ROPro ROCare RiskPro = FunPriOr

Method of estimation: Weighted Least Squares

Print residuals

Path Diagram

End of Problem

Sample Size =   274
```

Correlation Matrix

	Gtrust	GSDAmt	GSDCon	GSDHon	LOCIntr	LOCPOr
Gtrust	1.00					
GSDAmt	-0.04	1.00				
GSDCon	-0.07	0.41	1.00			
GSDHon	0.22	0.15	-0.07	1.00		
LOCIntr	0.19	-0.06	-0.01	0.23	1.00	
LOCPOr	-0.26	-0.12	0.17	-0.23	0.00	1.00
LOCChar	-0.31	-0.14	0.14	-0.29	-0.11	0.62
ROPro	-0.19	0.30	0.14	0.09	0.09	-0.04
ROCare	-0.05	0.14	0.05	-0.16	-0.01	-0.10
RiskPro	-0.24	0.15	0.04	0.00	-0.03	-0.02

Correlation Matrix

	LOCChar	ROPro	ROCare	RiskPro
LOCChar	1.00			
ROPro	0.04	1.00		
ROCare	0.02	0.36	1.00	
RiskPro	0.07	0.45	0.44	1.00

Number of Iterations = 14

LISREL Estimates (Weighted Least Squares)

Measurement Equations

Gtrust = 0.55*FunPriOr, Errorvar.= 0.70 , R^2 = 0.30
(0.043) (0.077)
12.73 9.11

GSDAmt = - 0.35*FunPriOr, Errorvar.= 0.88 , R^2 = 0.12
(0.047) (0.069)
-7.38 12.77

GSDCon = - 0.52*FunPriOr, Errorvar.= 0.73 , R^2 = 0.27
(0.045) (0.077)
-11.61 9.48

GSDHon = 0.37*FunPriOr, Errorvar.= 0.86 , R^2 = 0.14
(0.048) (0.070)
7.74 12.30

LOCIntr = 0.15*FunPriOr, Errorvar.= 0.98 , R^2 = 0.022
(0.052) (0.062)
2.85 15.67

LOCPOr = - 0.66*FunPriOr, Errorvar.= 0.56 , R^2 = 0.44
(0.037) (0.078)
-17.92 7.18

```
LOCChar =  - 0.77*FunPriOr, Errorvar.= 0.41  , R² = 0.59
            (0.034)                  (0.080)
            -22.63                    5.16

ROPro =  - 0.58*FunPriOr, Errorvar.= 0.67  , R² = 0.33
            (0.041)                  (0.077)
            -13.92                    8.67

ROCare =  - 0.48*FunPriOr, Errorvar.= 0.77  , R² = 0.23
            (0.044)                  (0.074)
            -10.88                    10.34

RiskPro =  - 0.58*FunPriOr, Errorvar.= 0.67  , R² = 0.33
            (0.041)                  (0.077)
            -14.12                    8.66
```

Correlation Matrix of Independent Variables

FunPriOr
1.00

Goodness of Fit Statistics

Degrees of Freedom = 35
Minimum Fit Function Chi-Square = 307.43 (P = 0.0)
Estimated Non-centrality Parameter (NCP) = 272.43
90 Percent Confidence Interval for NCP = (220.11 ; 332.24)
Minimum Fit Function Value = 1.13
Population Discrepancy Function Value (F0) = 1.00
90 Percent Confidence Interval for F0 = (0.81 ; 1.22)
Root Mean Square Error of Approximation (RMSEA) = 0.17
90 Percent Confidence Interval for RMSEA = (0.15 ; 0.19)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.00
Expected Cross-Validation Index (ECVI) = 1.27
90 Percent Confidence Interval for ECVI = (1.08 ; 1.49)
ECVI for Saturated Model = 0.40
ECVI for Independence Model = 2.87
Chi-Square for Independence Model with 45 Degrees of Freedom = 764.14
Independence AIC = 784.14
Model AIC = 347.43
Saturated AIC = 110.00
Independence CAIC = 830.27
Model CAIC = 439.70
Saturated CAIC = 363.72
Normed Fit Index (NFI) = 0.60
Non-Normed Fit Index (NNFI) = 0.51
Parsimony Normed Fit Index (PNFI) = 0.46
Comparative Fit Index (CFI) = 0.62
Incremental Fit Index (IFI) = 0.63
Relative Fit Index (RFI) = 0.48
Critical N (CN) = 51.92
Root Mean Square Residual (RMR) = 0.19
Standardized RMR = 0.19
Goodness of Fit Index (GFI) = 0.91
Adjusted Goodness of Fit Index (AGFI) = 0.86
Parsimony Goodness of Fit Index (PGFI) = 0.58

Fitted Covariance Matrix

	Gtrust	GSDAmt	GSDCon	GSDHon	LOCIntr	LOCPOr
Gtrust	1.00					
GSDAmt	-0.19	1.00				
GSDCon	-0.29	0.18	1.00			
GSDHon	0.20	-0.13	-0.19	1.00		
LOCIntr	0.08	-0.05	-0.08	0.05	1.00	
LOCPOr	-0.36	0.23	0.35	-0.25	-0.10	1.00
LOCChar	-0.42	0.27	0.40	-0.28	-0.11	0.51
ROPro	-0.32	0.20	0.30	-0.21	-0.09	0.38
ROCare	-0.26	0.17	0.25	-0.18	-0.07	0.32
RiskPro	-0.32	0.20	0.30	-0.21	-0.09	0.38

Fitted Covariance Matrix

	LOCChar	ROPro	ROCare	RiskPro
LOCChar	1.00			
ROPro	0.44	1.00		
ROCare	0.37	0.28	1.00	
RiskPro	0.44	0.33	0.28	1.00

Fitted Residuals

	Gtrust	GSDAmt	GSDCon	GSDHon	LOCIntr	LOCPOr
Gtrust	0.00					
GSDAmt	0.15	0.00				
GSDCon	0.22	0.23	0.00			
GSDHon	0.02	0.28	0.12	0.00		
LOCIntr	0.11	-0.01	0.07	0.17	0.00	
LOCPOr	0.11	-0.35	-0.17	0.02	0.09	0.00
LOCChar	0.12	-0.41	-0.26	0.00	0.00	0.11
ROPro	0.12	0.10	-0.16	0.30	0.18	-0.43
ROCare	0.21	-0.03	-0.20	0.02	0.06	-0.42
RiskPro	0.08	-0.05	-0.27	0.21	0.06	-0.40

Fitted Residuals

	LOCChar	ROPro	ROCare	RiskPro
LOCChar	0.00			
ROPro	-0.40	0.00		
ROCare	-0.35	0.08	0.00	
RiskPro	-0.38	0.12	0.16	0.00

Summary Statistics for Fitted Residuals

Smallest Fitted Residual =	-0.43
Median Fitted Residual =	0.00
Largest Fitted Residual =	0.30

Stemleaf Plot

```
 - 4|32100
 - 3|855
 - 2|760
 - 1|76
 - 0|531000000000000
   0|222667889
   1|011122225678
   2|11238
   3|0
```

Standardized Residuals

	Gtrust	GSDAmt	GSDCon	GSDHon	LOCIntr	LOCPOr
Gtrust	- -					
GSDAmt	2.85	- -				
GSDCon	4.35	5.78	- -			
GSDHon	0.35	5.17	2.33	- -		
LOCIntr	2.19	-0.22	1.31	3.20	- -	
LOCPOr	2.46	-7.02	-3.76	0.45	1.88	- -
LOCChar	2.98	-8.74	-5.78	-0.05	0.02	7.40
ROPro	2.59	2.12	-3.32	5.80	3.40	-8.47
ROCare	4.13	-0.55	-3.84	0.39	1.14	-8.32
RiskPro	1.72	-0.93	-5.22	4.06	1.10	-8.02

Standardized Residuals

	LOCChar	ROPro	ROCare	RiskPro
LOCChar	- -			
ROPro	-8.42	- -		
ROCare	-7.34	2.02	- -	
RiskPro	-7.90	3.65	4.57	- -

Summary Statistics for Standardized Residuals

```
Smallest Standardized Residual =   -8.74
  Median Standardized Residual =    0.02
 Largest Standardized Residual =    7.40
```

Stemleaf Plot

```
 - 8|75430
 - 6|930
 - 4|82
 - 2|883
 - 0|962100000000000
   0|34411379
   2|01235680246
   4|1146288
   6|4
```

Largest Negative Standardized Residuals

Residual for	LOCPOr	and GSDAmt	-7.02
Residual for	LOCPOr	and GSDCon	-3.76
Residual for	LOCChar	and GSDAmt	-8.74
Residual for	LOCChar	and GSDCon	-5.78
Residual for	ROPro	and GSDCon	-3.32
Residual for	ROPro	and LOCPOr	-8.47
Residual for	ROPro	and LOCChar	-8.42
Residual for	ROCare	and GSDCon	-3.84
Residual for	ROCare	and LOCPOr	-8.32
Residual for	ROCare	and LOCChar	-7.34
Residual for	RiskPro	and GSDCon	-5.22
Residual for	RiskPro	and LOCPOr	-8.02
Residual for	RiskPro	and LOCChar	-7.90

Largest Positive Standardized Residuals

Residual for	GSDAmt	and Gtrust	2.85
Residual for	GSDCon	and Gtrust	4.35
Residual for	GSDCon	and GSDAmt	5.78
Residual for	GSDHon	and GSDAmt	5.17
Residual for	LOCIntr	and GSDHon	3.20
Residual for	LOCChar	and Gtrust	2.98
Residual for	LOCChar	and LOCPOr	7.40
Residual for	ROPro	and Gtrust	2.59
Residual for	ROPro	and GSDHon	5.80
Residual for	ROPro	and LOCIntr	3.40
Residual for	ROCare	and Gtrust	4.13
Residual for	RiskPro	and GSDHon	4.06
Residual for	RiskPro	and ROPro	3.65
Residual for	RiskPro	and ROCare	4.57

The Modification Indices Suggest to Add an Error Covariance

Between	and	Decrease in Chi-Square	New Estimate
GSDCon	GSDAmt	81.4	0.50
GSDHon	GSDAmt	18.6	0.19
GSDHon	GSDCon	7.9	-0.14
LOCIntr	GSDAmt	16.2	-0.20
LOCIntr	GSDHon	11.9	0.18
LOCPOr	LOCIntr	10.0	0.14
LOCChar	GSDAmt	10.8	-0.13
LOCChar	LOCPOr	58.3	0.58
ROPro	LOCIntr	10.7	0.16
ROCare	Gtrust	16.6	0.19
ROCare	GSDHon	29.5	-0.27
RiskPro	GSDHon	8.4	0.13
RiskPro	ROCare	23.0	0.25

Time used: 0.125 Seconds

DATE: 11/15/2004
TIME: 10:57

L I S R E L 8.54

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140

Functional Privacy Orientation – Final Measurement Model

```
Measurement Model

Observed Variables:
Gtrust GSDAmt GSDCon GSDHon LOCIntr LOCPOr LOCChar ROPro
ROCare RiskPro IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC OWDSenT
ODTotT

Correlation Matrix from file FPOFin1115.cor
Asymptotic Covariance matrix from file FPOFin1115.acm

Sample Size = 274
Latent variable: FunPriOr

Relationships:
Gtrust GSDCon GSDHon LOCIntr LOCPOr LOCChar RiskPro = FunPriOr

Let the errors of LOCPOr and LOCChar covary

Method of estimation: Weighted Least Squares

Print residuals

Path Diagram

End of Problem

Sample Size =   274
```

Correlation Matrix

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	1.00					
GSDCon	-0.07	1.00				
GSDHon	0.22	-0.07	1.00			
LOCIntr	0.19	-0.01	0.23	1.00		
LOCPOr	-0.26	0.17	-0.23	0.00	1.00	
LOCChar	-0.31	0.14	-0.29	-0.11	0.62	1.00
RiskPro	-0.24	0.04	0.00	-0.03	-0.02	0.07

Correlation Matrix

	RiskPro
RiskPro	1.00

Number of Iterations = 10

LISREL Estimates (Weighted Least Squares)

Measurement Equations

Gtrust = 0.65*FunPriOr, Errorvar.= 0.58 , R^2 = 0.42
(0.070) (0.11)
9.24 5.34

GSDCon = - 0.18*FunPriOr, Errorvar.= 0.97 , R^2 = 0.034
(0.073) (0.066)
-2.53 14.61

GSDHon = 0.48*FunPriOr, Errorvar.= 0.77 , R^2 = 0.23
(0.067) (0.088)
7.15 8.74

LOCIntr = 0.31*FunPriOr, Errorvar.= 0.90 , R^2 = 0.098
(0.070) (0.075)
4.44 12.06

LOCPOr = - 0.46*FunPriOr, Errorvar.= 0.79 , R^2 = 0.21
(0.073) (0.090)
-6.29 8.83

LOCChar = - 0.55*FunPriOr, Errorvar.= 0.70 , R^2 = 0.30
(0.068) (0.096)
-8.00 7.27

RiskPro = - 0.23*FunPriOr, Errorvar.= 0.95 , R^2 = 0.051
(0.072) (0.069)
-3.14 13.83

Error Covariance for LOCChar and LOCPOr = 0.38
(0.065)
5.81

Goodness of Fit Statistics

Degrees of Freedom = 13
Minimum Fit Function Chi-Square = 30.44 (P = 0.0041)
Estimated Non-centrality Parameter (NCP) = 17.44
90 Percent Confidence Interval for NCP = (5.04 ; 37.53)
Minimum Fit Function Value = 0.11
Population Discrepancy Function Value (F0) = 0.064
90 Percent Confidence Interval for F0 = (0.018 ; 0.14)
Root Mean Square Error of Approximation (RMSEA) = 0.070
90 Percent Confidence Interval for RMSEA = (0.038 ; 0.10)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.14
Expected Cross-Validation Index (ECVI) = 0.22
90 Percent Confidence Interval for ECVI = (0.18 ; 0.29)
ECVI for Saturated Model = 0.21
ECVI for Independence Model = 1.40
Chi-Square for Independence Model with 21 Degrees of Freedom = 367.81
Independence AIC = 381.81
Model AIC = 60.44
Saturated AIC = 56.00
Independence CAIC = 414.10
Model CAIC = 129.64
Saturated CAIC = 185.17
Normed Fit Index (NFI) = 0.92
Non-Normed Fit Index (NNFI) = 0.92
Parsimony Normed Fit Index (PNFI) = 0.57
Comparative Fit Index (CFI) = 0.95
Incremental Fit Index (IFI) = 0.95
Relative Fit Index (RFI) = 0.87
Critical N (CN) = 249.34
Root Mean Square Residual (RMR) = 0.059
Standardized RMR = 0.059
Goodness of Fit Index (GFI) = 0.99
Adjusted Goodness of Fit Index (AGFI) = 0.97
Parsimony Goodness of Fit Index (PGFI) = 0.46

Fitted Covariance Matrix

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	1.00					
GSDCon	-0.12	1.00				
GSDHon	0.31	-0.09	1.00			
LOCIntr	0.20	-0.06	0.15	1.00		
LOCPOr	-0.30	0.08	-0.22	-0.14	1.00	
LOCChar	-0.35	0.10	-0.26	-0.17	0.63	1.00
RiskPro	-0.15	0.04	-0.11	-0.07	0.10	0.12

Fitted Covariance Matrix

	RiskPro
RiskPro	1.00

Fitted Residuals

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	0.00					
GSDCon	0.05	0.00				
GSDHon	-0.09	0.02	0.00			
LOCIntr	-0.01	0.05	0.08	0.00		
LOCPOr	0.04	0.09	-0.01	0.14	0.00	
LOCChar	0.05	0.04	-0.02	0.06	-0.01	0.00
RiskPro	-0.09	0.00	0.10	0.04	-0.12	-0.06

Fitted Residuals

	RiskPro
RiskPro	0.00

Summary Statistics for Fitted Residuals

Smallest Fitted Residual = -0.12
Median Fitted Residual = 0.00
Largest Fitted Residual = 0.14

Stemleaf Plot

```
- 1|2
- 0|996
- 0|211100000000
  0|2444
  0|555689
  1|04
```

Standardized Residuals

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	- -					
GSDCon	1.43	- -				
GSDHon	-3.61	0.33	- -			
LOCIntr	-0.37	0.93	1.87	- -		
LOCPOr	1.56	1.94	-0.20	2.93	- -	
LOCChar	2.37	0.95	-0.89	1.44	-1.25	- -
RiskPro	-3.20	-0.08	2.18	0.78	-2.52	-1.33

Standardized Residuals

	RiskPro
RiskPro	- -

```
 Summary Statistics for Standardized Residuals

 Smallest Standardized Residual =   -3.61
   Median Standardized Residual =    0.00
  Largest Standardized Residual =    2.93

 Stemleaf Plot

 - 3|62
 - 2|5
 - 1|33
 - 0|94210000000
   0|3899
   1|44699
   2|249


 Largest Negative Standardized Residuals
 Residual for GSDHon  and Gtrust  -3.61
 Residual for RiskPro and Gtrust  -3.20

Largest Positive Standardized Residuals
 Residual for LOCPOr and LOCIntr   2.93

 The Modification Indices Suggest to Add an Error Covariance
  Between    and     Decrease in Chi-Square    New Estimate
 RiskPro   Gtrust             12.1                -0.25

                           Time used:    0.063 Seconds
```

DATE: 11/15/2004
TIME: 12:30

L I S R E L 8.54

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140

Online Privacy Orientation – Measurement Model

```
Observed Variables:
Gtrust GSDAmt GSDCon GSDHon LOCIntr LOCPOr LOCChar ROPro ROCare
RiskPro IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC OWDSenT ODTotT

Correlation Matrix from file ODFinal1115.cor
Asymptotic Covariance Matrix from file ODFinal1115.acm

Sample Size = 274

Latent variable: OnLinePO

Relationships:
IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC OWDSenT ODTotT = OnLinePO

Method of estimation: Weighted Least Squares

Print residuals

Path Diagram

End of Problem

Sample Size =   274
```

Correlation Matrix

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	1.00					
IMPCCol	0.50	1.00				
IMPCIA	0.61	0.58	1.00			
IMPCUSU	0.49	0.51	0.72	1.00		
LevPrivC	0.08	0.17	0.06	0.00	1.00	
OWDSenT	-0.15	-0.25	-0.15	-0.15	-0.16	1.00
ODTotT	-0.06	-0.25	-0.04	-0.03	-0.21	0.03

Correlation Matrix

	ODTotT
ODTotT	1.00

Number of Iterations = 6

LISREL Estimates (Weighted Least Squares)

Measurement Equations

IMPCErr = 0.70*OnLineDi, Errorvar.= 0.51 , R² = 0.49
(0.036) (0.079)
19.42 6.55

IMPCCol = 0.77*OnLineDi, Errorvar.= 0.41 , R² = 0.59
(0.033) (0.079)
23.48 5.21

IMPCIA = 0.91*OnLineDi, Errorvar.= 0.18 , R² = 0.82
(0.022) (0.073)
40.94 2.46

IMPCUSU = 0.80*OnLineDi, Errorvar.= 0.36 , R² = 0.64
(0.029) (0.076)
27.89 4.69

LevPrivC = 0.14*OnLineDi, Errorvar.= 0.98 , R² = 0.021
(0.061) (0.063)
2.38 15.54

OWDSenT = - 0.25*OnLineDi, Errorvar.= 0.94 , R² = 0.064
(0.059) (0.067)
-4.31 13.89

ODTotT = - 0.16*OnLineDi, Errorvar.= 0.97 , R² = 0.026
(0.060) (0.064)
-2.70 15.31

Goodness of Fit Statistics

Degrees of Freedom = 14
Minimum Fit Function Chi-Square = 51.07 (P = 0.00)
Estimated Non-centrality Parameter (NCP) = 37.07
90 Percent Confidence Interval for NCP = (18.91 ; 62.81)
Minimum Fit Function Value = 0.19
Population Discrepancy Function Value (F0) = 0.14
90 Percent Confidence Interval for F0 = (0.069 ; 0.23)
Root Mean Square Error of Approximation (RMSEA) = 0.098
90 Percent Confidence Interval for RMSEA = (0.070 ; 0.13)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.0033
Expected Cross-Validation Index (ECVI) = 0.29
90 Percent Confidence Interval for ECVI = (0.22 ; 0.38)
ECVI for Saturated Model = 0.21
ECVI for Independence Model = 3.35
Chi-Square for Independence Model with 21 Degrees of Freedom = 901.24
Independence AIC = 915.24
Model AIC = 79.07
Saturated AIC = 56.00
Independence CAIC = 947.53
Model CAIC = 143.65
Saturated CAIC = 185.17
Normed Fit Index (NFI) = 0.94
Non-Normed Fit Index (NNFI) = 0.94
Parsimony Normed Fit Index (PNFI) = 0.63
Comparative Fit Index (CFI) = 0.96
Incremental Fit Index (IFI) = 0.96
Relative Fit Index (RFI) = 0.92
Critical N (CN) = 156.80
Root Mean Square Residual (RMR) = 0.075
Standardized RMR = 0.075
Goodness of Fit Index (GFI) = 0.98
Adjusted Goodness of Fit Index (AGFI) = 0.96
Parsimony Goodness of Fit Index (PGFI) = 0.49

Fitted Covariance Matrix

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	1.00					
IMPCCol	0.54	1.00				
IMPCIA	0.63	0.70	1.00			
IMPCUSU	0.56	0.62	0.73	1.00		
LevPrivC	0.10	0.11	0.13	0.12	1.00	
OWDSenT	-0.18	-0.19	-0.23	-0.20	-0.04	1.00
ODTotT	-0.11	-0.12	-0.15	-0.13	-0.02	0.04

Fitted Covariance Matrix

	ODTotT
ODTotT	1.00

Fitted Residuals

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	0.00					
IMPCCol	-0.04	0.00				
IMPCIA	-0.02	-0.11	0.00			
IMPCUSU	-0.07	-0.10	-0.01	0.00		
LevPrivC	-0.02	0.06	-0.07	-0.12	0.00	
OWDSenT	0.03	-0.06	0.08	0.05	-0.12	0.00
ODTotT	0.05	-0.13	0.11	0.10	-0.19	-0.01

Fitted Residuals

	ODTotT
ODTotT	0.00

Summary Statistics for Fitted Residuals

Smallest Fitted Residual = -0.19
Median Fitted Residual = 0.00
Largest Fitted Residual = 0.11

Stemleaf Plot

```
- 1|9
- 1|32210
- 0|776
- 0|422110000000
  0|3
  0|5568
  1|01
```

Standardized Residuals

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	- -					
IMPCCol	-1.49	- -				
IMPCIA	-1.95	-5.53	- -			
IMPCUSU	-2.67	-4.04	-1.54	- -		
LevPrivC	-0.48	1.71	-2.72	-3.35	- -	
OWDSenT	0.72	-1.72	3.17	1.46	-2.14	- -
ODTotT	1.17	-4.15	4.27	2.76	-3.36	-0.16

Standardized Residuals

	ODTotT
ODTotT	- -

Summary Statistics for Standardized Residuals

Smallest Standardized Residual = -5.53
Median Standardized Residual = -0.08
Largest Standardized Residual = 4.27

Stemleaf Plot

```
- 5|5
- 4|20
- 3|44
- 2|771
- 1|9755
- 0|520000000
  0|7
  1|257
  2|8
  3|2
  4|3
```

Largest Negative Standardized Residuals

Residual for	IMPCIA	and	IMPCCol	-5.53
Residual for	IMPCUSU	and	IMPCErr	-2.67
Residual for	IMPCUSU	and	IMPCCol	-4.04
Residual for	LevPrivC	and	IMPCIA	-2.72
Residual for	LevPrivC	and	IMPCUSU	-3.35
Residual for	ODTotT	and	IMPCCol	-4.15
Residual for	ODTotT	and	LevPrivC	-3.36

Largest Positive Standardized Residuals

Residual for	OWDSenT	and	IMPCIA	3.17
Residual for	ODTotT	and	IMPCIA	4.27
Residual for	ODTotT	and	IMPCUSU	2.76

The Modification Indices Suggest to Add an Error Covariance

Between	and	Decrease in Chi-Square	New Estimate
ODTotT	IMPCCol	15.8	-0.18
ODTotT	LevPrivC	8.5	-0.16

Time used: 0.063 Seconds

DATE: 12/ 6/2004
TIME: 21:37

L I S R E L 8.54

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140

Privacy Orientation: Grams 12 04 2004

Full Structural Model with Measurement Models – Initial

Observed Variables:
Gtrust GSDAmt GSDCon GSDHon LOCIntr LOCPOr LOCChar RiskPro Careless
RiskOri IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC OWDSenT ODTotT

Correlation Matrix from file StruMod1206.cor
Asymptotic Covariance Matrix from file StruMod1206.acm
!Covariance Matrix from file StruMod1206nn.cov

Sample Size = 274

Latent variables: OnLineDis FunPriOr

Relationships:
IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC OWDSenT ODTotT = OnLineDis
Gtrust GSDHon LOCIntr LOCPOr LOCChar RiskOri = FunPriOr

! Structural Model

FunPriOr -> OnLineDis

Method of estimation: Weighted Least Squares
Print Residuals
Lisrel Output: SS SC MI
Path Diagram TV=5
End of Problem

Correlation Matrix

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	1.00					
IMPCCol	0.11	1.00				
IMPCIA	0.09	0.50	1.00			
IMPCUSU	0.14	0.61	0.58	1.00		
LevPrivC	0.11	0.49	0.52	0.73	1.00	
OWDSenT	-0.10	0.08	0.17	0.07	-0.01	1.00
ODTotT	0.02	0.15	0.25	0.15	0.15	0.16
Gtrust	-0.24	-0.02	0.01	-0.04	-0.08	0.20
GSDHon	0.13	-0.05	0.08	0.05	0.08	0.11
LOCIntr	0.00	-0.10	0.02	-0.05	-0.09	0.01
LOCPOr	-0.03	-0.08	-0.07	-0.04	-0.05	0.02
LOCChar	-0.02	0.08	0.03	0.05	0.08	0.05
RiskOri	0.44	0.12	0.11	0.12	0.16	-0.03

Correlation Matrix

	ODTotT	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar
ODTotT	1.00					
Gtrust	0.08	1.00				
GSDHon	0.06	-0.07	1.00			
LOCIntr	-0.08	0.22	0.08	1.00		
LOCPOr	0.01	0.19	-0.05	0.23	1.00	
LOCChar	0.06	-0.26	0.01	-0.23	0.00	1.00
RiskOri	-0.02	-0.05	0.11	-0.16	-0.01	-0.10

Correlation Matrix

	RiskOri
RiskOri	1.00

Privacy Orientation: Grams 12 04 2004

Parameter Specifications

LAMBDA-Y

	OnLineDi
IMPCErr	0
IMPCCol	1
IMPCIA	2
IMPCUSU	3
LevPrivC	4
OWDSenT	5
ODTotT	6

LAMBDA-X

	FunPriOr
Gtrust	7
GSDHon	8
LOCIntr	9
LOCPOr	10
LOCChar	11
RiskOri	12

GAMMA

	FunPriOr
OnLineDi	13

PSI

OnLineDi
14

THETA-EPS

IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
15	16	17	18	19	20

THETA-EPS

ODTotT
21

THETA-DELTA

Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
22	23	24	25	26	27

Number of Iterations =142

LISREL Estimates (Weighted Least Squares)

LAMBDA-Y

	OnLineDi
IMPCErr	0.07
IMPCCol	0.71 (0.55) 1.28

IMPCIA	0.72
	(0.56)
	1.28
IMPCUSU	0.91
	(0.71)
	1.28
LevPrivC	0.82
	(0.64)
	1.28
OWDSenT	0.09
	(0.10)
	0.96
ODTotT	0.26
	(0.21)
	1.25

LAMBDA-X

	FunPriOr
Gtrust	0.59
	(0.06)
	9.24
GSDHon	-0.02
	(0.07)
	-0.30
LOCIntr	0.66
	(0.07)
	9.51
LOCPOr	0.36
	(0.07)
	5.48
LOCChar	-0.49
	(0.06)
	-7.61
RiskOri	-0.01
	(0.06)
	-0.20

GAMMA

	FunPriOr
OnLineDi	-0.13
	(0.13)
	-0.99

Covariance Matrix of ETA and KSI

	OnLineDi	FunPriOr
OnLineDi	1.00	
FunPriOr	-0.13	1.00

PHI

FunPriOr
1.00

PSI

OnLineDi
0.98
(1.54)
0.64

Squared Multiple Correlations for Structural Equations

OnLineDi
0.02

Squared Multiple Correlations for Reduced Form

OnLineDi
0.02

THETA-EPS

IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
1.00	0.50	0.48	0.17	0.33	0.99
(0.06)	(0.08)	(0.08)	(0.07)	(0.08)	(0.06)
16.33	6.42	6.19	2.32	4.38	16.13

THETA-EPS

ODTotT
0.93
(0.07)
13.85

Squared Multiple Correlations for Y - Variables

IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
0.00	0.50	0.52	0.83	0.67	0.01

Squared Multiple Correlations for Y - Variables

ODTotT
0.07

THETA-DELTA

Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
0.65	1.00	0.57	0.87	0.76	1.00
(0.10)	(0.06)	(0.11)	(0.08)	(0.09)	(0.06)
6.64	16.50	5.25	11.41	8.73	16.51

Squared Multiple Correlations for X - Variables

Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
0.35	0.00	0.43	0.13	0.24	0.00

Goodness of Fit Statistics

Degrees of Freedom = 64
Minimum Fit Function Chi-Square = 257.97 (P = 0.0)
Estimated Non-centrality Parameter (NCP) = 193.97
90 Percent Confidence Interval for NCP = (148.25 ; 247.25)

Minimum Fit Function Value = 0.94
Population Discrepancy Function Value (F0) = 0.71
90 Percent Confidence Interval for F0 = (0.54 ; 0.91)
Root Mean Square Error of Approximation (RMSEA) = 0.11
90 Percent Confidence Interval for RMSEA = (0.092 ; 0.12)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.00

Expected Cross-Validation Index (ECVI) = 1.14
90 Percent Confidence Interval for ECVI = (0.98 ; 1.34)
ECVI for Saturated Model = 0.67
ECVI for Independence Model = 4.84

Chi-Square for Independence Model with 78 Degrees of Freedom = 1294.24
Independence AIC = 1320.24
Model AIC = 311.97
Saturated AIC = 182.00
Independence CAIC = 1380.21
Model CAIC = 436.52

Saturated CAIC = 601.79

Normed Fit Index (NFI) = 0.80
Non-Normed Fit Index (NNFI) = 0.81
Parsimony Normed Fit Index (PNFI) = 0.66
Comparative Fit Index (CFI) = 0.84
Incremental Fit Index (IFI) = 0.84
Relative Fit Index (RFI) = 0.76

Critical N (CN) = 99.65

Root Mean Square Residual (RMR) = 0.086
Standardized RMR = 0.086
Goodness of Fit Index (GFI) = 0.95
Adjusted Goodness of Fit Index (AGFI) = 0.92
Parsimony Goodness of Fit Index (PGFI) = 0.67

Fitted Covariance Matrix

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	1.00					
IMPCCol	0.05	1.00				
IMPCIA	0.05	0.51	1.00			
IMPCUSU	0.06	0.64	0.65	1.00		
LevPrivC	0.06	0.58	0.59	0.75	1.00	
OWDSenT	0.01	0.06	0.07	0.08	0.07	1.00
ODTotT	0.02	0.18	0.18	0.23	0.21	0.02
Gtrust	-0.01	-0.05	-0.05	-0.07	-0.06	-0.01
GSDHon	0.00	0.00	0.00	0.00	0.00	0.00
LOCIntr	-0.01	-0.06	-0.06	-0.07	-0.07	-0.01
LOCPOr	0.00	-0.03	-0.03	-0.04	-0.04	0.00
LOCChar	0.00	0.04	0.04	0.06	0.05	0.01
RiskOri	0.00	0.00	0.00	0.00	0.00	0.00

Fitted Covariance Matrix

	ODTotT	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar
ODTotT	1.00					
Gtrust	-0.02	1.00				
GSDHon	0.00	-0.01	1.00			
LOCIntr	-0.02	0.39	-0.01	1.00		
LOCPOr	-0.01	0.21	-0.01	0.23	1.00	
LOCChar	0.02	-0.29	0.01	-0.32	-0.17	1.00
RiskOri	0.00	-0.01	0.00	-0.01	0.00	0.01

Fitted Covariance Matrix

	RiskOri
RiskOri	1.00

Fitted Residuals

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	0.00					
IMPCCol	0.06	0.00				
IMPCIA	0.04	-0.01	0.00			
IMPCUSU	0.08	-0.04	-0.07	0.00		
LevPrivC	0.05	-0.09	-0.07	-0.02	0.00	
OWDSenT	-0.11	0.02	0.11	-0.02	-0.08	0.00
ODTotT	0.00	-0.04	0.06	-0.09	-0.06	0.13
Gtrust	-0.23	0.03	0.06	0.03	-0.02	0.21
GSDHon	0.13	-0.05	0.08	0.05	0.07	0.11
LOCIntr	0.00	-0.04	0.08	0.02	-0.03	0.01
LOCPOr	-0.03	-0.05	-0.04	0.00	-0.02	0.02
LOCChar	-0.02	0.03	-0.02	0.00	0.03	0.05
RiskOri	0.44	0.12	0.11	0.12	0.16	-0.03

Fitted Residuals

	ODTotT	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar
ODTotT	0.00					
Gtrust	0.10	0.00				
GSDHon	0.06	-0.06	0.00			
LOCIntr	-0.06	-0.17	0.09	0.00		
LOCPOr	0.02	-0.02	-0.05	-0.01	0.00	
LOCChar	0.05	0.03	0.00	0.09	0.17	0.00
RiskOri	-0.02	-0.04	0.11	-0.15	0.00	-0.10

Fitted Residuals

	RiskOri
RiskOri	0.00

Summary Statistics for Fitted Residuals

```
Smallest Fitted Residual =   -0.23
  Median Fitted Residual =    0.00
 Largest Fitted Residual =    0.44
```

Stemleaf Plot

```
- 2|3
- 1|7510
- 0|998776665554444433322222222110000000000000000000
  0|12222333334555566667888 99
  1|01111223367
  2|1
  3|
  4|4
```

Standardized Residuals

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	- -					
IMPCCol	1.35	- -				
IMPCIA	0.81	-0.28	- -			
IMPCUSU	2.21	-2.49	-4.00	- -		
LevPrivC	1.33	-3.24	-2.79	-2.11	- -	
OWDSenT	-1.86	0.37	2.60	-0.64	-2.27	- -
ODTotT	0.06	-0.85	1.77	-3.25	-1.67	2.35
Gtrust	-4.13	0.58	1.24	0.55	-0.36	3.65
GSDHon	2.12	-0.82	1.31	0.87	1.23	1.79
LOCIntr	0.04	-0.82	1.58	0.49	-0.60	0.22
LOCPOr	-0.41	-0.93	-0.66	-0.06	-0.27	0.39
LOCChar	-0.41	0.62	-0.28	-0.03	0.53	0.81
RiskOri	8.90	1.95	1.84	2.02	2.68	-0.48

Standardized Residuals

	ODTotT	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar
ODTotT	- -					
Gtrust	1.74	- -				
GSDHon	0.96	-1.33	- -			
LOCIntr	-0.98	-5.95	2.23	- -		
LOCPOr	0.31	-0.59	-0.84	-0.29	- -	
LOCChar	0.81	1.13	0.06	3.39	3.62	- -
RiskOri	-0.37	-0.91	1.85	-3.50	-0.07	-2.02

Standardized Residuals

	RiskOri
RiskOri	- -

Summary Statistics for Standardized Residuals

Smallest Standardized Residual = -5.95
Median Standardized Residual = 0.00
Largest Standardized Residual = 8.90

Stemleaf Plot

```
- 4|910
- 2|52285310
- 0|9730999888766654444333311000000000000000
  0|11234455666888901223336788889
  2|0122367466
  4|
  6|
  8|9
```

Largest Negative Standardized Residuals
Residual for IMPCUSU and   IMPCIA -4.00
Residual for LevPrivC and IMPCCol -3.24
Residual for LevPrivC and   IMPCIA -2.79
Residual for   ODTotT and IMPCUSU -3.25
Residual for   Gtrust and IMPCErr -4.13
Residual for LOCIntr and   Gtrust -5.95
Residual for RiskOri and LOCIntr -3.50
Largest Positive Standardized Residuals
Residual for OWDSenT and   IMPCIA   2.60
Residual for   Gtrust and OWDSenT   3.65
Residual for LOCChar and LOCIntr   3.39
Residual for LOCChar and   LOCPOr   3.62
Residual for RiskOri and IMPCErr   8.90
Residual for RiskOri and LevPrivC   2.68

Modification Indices and Expected Change

No Non-Zero Modification Indices for LAMBDA-Y
No Non-Zero Modification Indices for LAMBDA-X
No Non-Zero Modification Indices for BETA
No Non-Zero Modification Indices for GAMMA
No Non-Zero Modification Indices for PHI
No Non-Zero Modification Indices for PSI

Modification Indices for THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	- -					
IMPCCol	0.33	- -				
IMPCIA	1.18	2.81	- -			
IMPCUSU	3.70	0.58	4.18	- -		
LevPrivC	6.55	4.74	0.06	7.41	- -	
OWDSenT	1.39	0.04	3.60	0.41	5.98	- -
ODTotT	7.98	0.15	6.14	3.85	0.23	1.09

Modification Indices for THETA-EPS

	ODTotT
ODTotT	- -

Expected Change for THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	- -					
IMPCCol	0.02	- -				
IMPCIA	-0.04	0.07	- -			
IMPCUSU	0.06	0.03	-0.08	- -		
LevPrivC	-0.09	-0.08	0.01	0.16	- -	
OWDSenT	-0.06	0.01	0.08	0.02	-0.09	- -
ODTotT	0.14	-0.02	0.11	-0.07	0.02	0.06

Expected Change for THETA-EPS

	ODTotT
ODTotT	- -

Completely Standardized Expected Change for THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
IMPCErr	- -					
IMPCCol	0.02	- -				
IMPCIA	-0.04	0.07	- -			
IMPCUSU	0.06	0.03	-0.08	- -		
LevPrivC	-0.09	-0.08	0.01	0.16	- -	
OWDSenT	-0.06	0.01	0.08	0.02	-0.09	- -
ODTotT	0.14	-0.02	0.11	-0.07	0.02	0.06

Completely Standardized Expected Change for THETA-EPS

	ODTotT
ODTotT	- -

Modification Indices for THETA-DELTA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
Gtrust	28.76	0.10	0.40	0.88	0.26	9.11
GSDHon	0.12	4.83	0.00	0.20	0.98	7.00
LOCIntr	17.30	0.34	7.77	0.04	0.16	0.10
LOCPOr	0.20	1.31	1.32	0.51	0.01	0.00
LOCChar	0.70	1.49	0.10	0.53	1.41	3.03
RiskOri	108.85	0.32	3.25	3.73	6.24	0.56

Modification Indices for THETA-DELTA-EPS

	ODTotT
Gtrust	3.51
GSDHon	1.00
LOCIntr	6.99
LOCPOr	0.68
LOCChar	0.11
RiskOri	8.68

Expected Change for THETA-DELTA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
Gtrust	-0.25	0.01	-0.03	0.03	-0.02	0.15
GSDHon	0.02	-0.10	0.00	0.02	0.04	0.14
LOCIntr	0.20	-0.02	0.12	-0.01	-0.01	-0.02
LOCPOr	-0.02	-0.05	-0.05	0.02	0.00	0.00
LOCChar	0.04	0.05	-0.01	-0.02	0.04	0.09
RiskOri	0.46	0.02	0.07	-0.06	0.09	0.04

Expected Change for THETA-DELTA-EPS

	ODTotT
Gtrust	0.10
GSDHon	0.06
LOCIntr	-0.14
LOCPOr	0.05
LOCChar	0.02
RiskOri	-0.15

Completely Standardized Expected Change for THETA-DELTA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
Gtrust	-0.25	0.01	-0.03	0.03	-0.02	0.15
GSDHon	0.02	-0.10	0.00	0.02	0.04	0.14
LOCIntr	0.20	-0.02	0.12	-0.01	-0.01	-0.02
LOCPOr	-0.02	-0.05	-0.05	0.02	0.00	0.00
LOCChar	0.04	0.05	-0.01	-0.02	0.04	0.09
RiskOri	0.46	0.02	0.07	-0.06	0.09	0.04

Completely Standardized Expected Change for THETA-DELTA-EPS

	ODTotT
Gtrust	0.10
GSDHon	0.06
LOCIntr	-0.14
LOCPOr	0.05
LOCChar	0.02
RiskOri	-0.15

Modification Indices for THETA-DELTA

	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
Gtrust	- -					
GSDHon	1.89	- -				
LOCIntr	6.83	7.54	- -			
LOCPOr	0.61	2.38	6.26	- -		
LOCChar	6.04	0.26	0.34	11.84	- -	
RiskOri	15.91	2.56	46.80	4.06	8.02	- -

Expected Change for THETA-DELTA

	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
Gtrust	- -					
GSDHon	-0.08	- -				
LOCIntr	-0.32	0.17	- -			
LOCPOr	0.05	-0.09	0.20	- -		
LOCChar	-0.24	0.03	-0.06	0.19	- -	
RiskOri	0.21	0.08	-0.38	0.10	-0.15	- -

Completely Standardized Expected Change for THETA-DELTA

	Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
Gtrust	- -					
GSDHon	-0.08	- -				
LOCIntr	-0.32	0.17	- -			
LOCPOr	0.05	-0.09	0.20	- -		
LOCChar	-0.24	0.03	-0.06	0.19	- -	
RiskOri	0.21	0.08	-0.38	0.10	-0.15	- -

Maximum Modification Index is 108.85 for Element (6, 1) of THETA DELTA-EPSILON

Standardized Solution

LAMBDA-Y

	OnLineDi
IMPCErr	0.07
IMPCCol	0.71
IMPCIA	0.72
IMPCUSU	0.91
LevPrivC	0.82
OWDSenT	0.09
ODTotT	0.26

LAMBDA-X

	FunPriOr
Gtrust	0.59
GSDHon	-0.02
LOCIntr	0.66
LOCPOr	0.36
LOCChar	-0.49
RiskOri	-0.01

GAMMA

	FunPriOr
OnLineDi	-0.13

Correlation Matrix of ETA and KSI

	OnLineDi	FunPriOr
OnLineDi	1.00	
FunPriOr	-0.13	1.00

PSI

	OnLineDi
	0.98

Regression Matrix ETA on KSI (Standardized)

	FunPriOr
OnLineDi	-0.13

Completely Standardized Solution

LAMBDA-Y

	OnLineDi
IMPCErr	0.07
IMPCCol	0.71
IMPCIA	0.72
IMPCUSU	0.91
LevPrivC	0.82
OWDSenT	0.09
ODTotT	0.26

LAMBDA-X

	FunPriOr
Gtrust	0.59
GSDHon	-0.02
LOCIntr	0.66
LOCPOr	0.36
LOCChar	-0.49
RiskOri	-0.01

GAMMA

	FunPriOr
OnLineDi	-0.13

Correlation Matrix of ETA and KSI

	OnLineDi	FunPriOr
OnLineDi	1.00	
FunPriOr	-0.13	1.00

PSI

	OnLineDi
	0.98

THETA-EPS

IMPCErr	IMPCCol	IMPCIA	IMPCUSU	LevPrivC	OWDSenT
1.00	0.50	0.48	0.17	0.33	0.99

THETA-EPS

ODTotT
0.93

THETA-DELTA

Gtrust	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskOri
0.65	1.00	0.57	0.87	0.76	1.00

Regression Matrix ETA on KSI (Standardized)

	FunPriOr
OnLineDi	-0.13

Time used: 0.281 Seconds

DATE: 12/14/2004
TIME: 20:37

L I S R E L 8.54

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140

Privacy Orientation: Grams 12 04 2004

Full Structural Model with Measurement Models – Final

```
Observed Variables:
Gtrust GSDAmt GSDCon GSDHon LOCIntr LOCPOr LOCChar
ROPro ROCare RiskPro IMPCErr IMPCCol IMPCIA IMPCUSU LevPrivC
OWDSenT ODTotT

Correlation Matrix from file StruModNor1111.cor
Asymptotic Covariance Matrix from file StruModNor1111.acm

Sample Size = 274

Latent variables: OnLinePO FunPriOr

Relationships:
IMPCErr IMPCCol IMPCIA IMPCUSU OWDSenT = OnLinePO
Gtrust GSDCon GSDHon LOCIntr LOCPOr LOCChar RiskPro = FunPriOr

! Structural Model

FunPriOr -> OnLinePO

let the errors of LOCPOr and LOCChar covary
let the errors of IMPCCol and OWDSenT covary

Method of estimation: Weighted Least Squares
Print Residuals
Lisrel output: RS MI SS SC EF
Path Diagram TV=5
End of Problem
```

Correlation Matrix

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT	Gtrust
IMPCErr	1.00					
IMPCCol	0.50	1.00				
IMPCIA	0.61	0.58	1.00			
IMPCUSU	0.49	0.51	0.72	1.00		
OWDSenT	-0.15	-0.25	-0.15	-0.15	1.00	
Gtrust	0.02	-0.01	0.04	0.09	0.08	1.00
GSDCon	0.07	-0.02	0.02	-0.04	0.01	-0.07
GSDHon	0.10	-0.02	0.05	0.10	-0.08	0.22
LOCIntr	0.08	0.07	0.04	0.06	0.01	0.19
LOCPOr	-0.08	-0.03	-0.05	-0.07	0.06	-0.26
LOCChar	-0.05	-0.05	-0.08	-0.15	0.05	-0.31
RiskPro	-0.11	-0.09	-0.14	-0.12	0.02	-0.24

Correlation Matrix

	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskPro
GSDCon	1.00					
GSDHon	-0.07	1.00				
LOCIntr	-0.01	0.23	1.00			
LOCPOr	0.17	-0.23	0.00	1.00		
LOCChar	0.14	-0.29	-0.11	0.62	1.00	
RiskPro	0.04	0.00	-0.03	-0.02	0.07	1.00

Parameter Specifications

LAMBDA-Y

	OnLinePO
IMPCErr	0
IMPCCol	1
IMPCIA	2
IMPCUSU	3
OWDSenT	4

LAMBDA-X

	FunPriOr
Gtrust	5
GSDCon	6
GSDHon	7
LOCIntr	8
LOCPOr	9
LOCChar	10
RiskPro	11

GAMMA

	FunPriOr
OnLinePO	12

PSI

	OnLinePO
	13

THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
IMPCErr	14				
IMPCCol	0	15			
IMPCIA	0	0	16		
IMPCUSU	0	0	0	17	
OWDSenT	0	18	0	0	19

THETA-DELTA

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	20					
GSDCon	0	21				
GSDHon	0	0	22			
LOCIntr	0	0	0	23		
LOCPOr	0	0	0	0	24	
LOCChar	0	0	0	0	25	26
RiskPro	0	0	0	0	0	0

THETA-DELTA

	RiskPro
RiskPro	27

Number of Iterations = 12

LISREL Estimates (Weighted Least Squares)

LAMBDA-Y

	OnLinePO
IMPCErr	0.70
IMPCCol	0.69 (0.05) 14.73

IMPCIA	0.90
	(0.05)
	17.23
IMPCUSU	0.81
	(0.05)
	17.41
OWDSenT	-0.17
	(0.06)
	-2.78

LAMBDA-X

	FunPriOr
Gtrust	0.66
	(0.07)
	9.91
GSDCon	-0.18
	(0.07)
	-2.59
GSDHon	0.47
	(0.06)
	7.39
LOCIntr	0.32
	(0.07)
	4.73
LOCPOr	-0.46
	(0.07)
	-6.65
LOCChar	-0.54
	(0.07)
	-8.34
RiskPro	-0.26
	(0.07)
	-3.82

GAMMA

	FunPriOr
OnLinePO	0.19
	(0.08)
	2.51

Covariance Matrix of ETA and KSI

	OnLinePO	FunPriOr
OnLinePO	1.00	
FunPriOr	0.19	1.00

PHI

	FunPriOr
	1.00

PSI

	OnLinePO
	0.96
	(0.10)
	9.42

Squared Multiple Correlations for Structural Equations

	OnLinePO
	0.04

Squared Multiple Correlations for Reduced Form

	OnLinePO
	0.04

THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
IMPCErr	0.51				
	(0.08)				
	6.50				
IMPCCol	- -	0.53			
		(0.08)			
		6.72			
IMPCIA	- -	- -	0.19		
			(0.07)		
			2.56		
IMPCUSU	- -	- -	- -	0.34	
				(0.08)	
				4.41	
OWDSenT	- -	-0.14	- -	- -	0.97
		(0.05)			(0.06)
		-2.99			15.20

Squared Multiple Correlations for Y - Variables

IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
0.49	0.47	0.81	0.66	0.03

THETA-DELTA

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	0.56 (0.11) 5.22					
GSDCon	- -	0.97 (0.07) 14.73				
GSDHon	- -	- -	0.78 (0.09) 9.06			
LOCIntr	- -	- -	- -	0.90 (0.07) 12.01		
LOCPOr	- -	- -	- -	- -	0.79 (0.09) 8.94	
LOCChar	- -	- -	- -	- -	0.39 (0.06) 6.27	0.71 (0.09) 7.59
RiskPro	- -	- -	- -	- -	- -	- -

THETA-DELTA

	RiskPro
RiskPro	0.93 (0.07) 13.14

Squared Multiple Correlations for X - Variables

Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
0.44	0.03	0.22	0.10	0.21	0.29

Squared Multiple Correlations for X - Variables

RiskPro
0.07

Goodness of Fit Statistics

Degrees of Freedom = 51
Minimum Fit Function Chi-Square = 74.82 (P = 0.017)
Estimated Non-centrality Parameter (NCP) = 23.82
90 Percent Confidence Interval for NCP = (4.63 ; 51.00)

Minimum Fit Function Value = 0.27
Population Discrepancy Function Value (F0) = 0.087
90 Percent Confidence Interval for F0 = (0.017 ; 0.19)
Root Mean Square Error of Approximation (RMSEA) = 0.041
90 Percent Confidence Interval for RMSEA = (0.018 ; 0.061)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.75

Expected Cross-Validation Index (ECVI) = 0.47
90 Percent Confidence Interval for ECVI = (0.40 ; 0.57)
ECVI for Saturated Model = 0.57
ECVI for Independence Model = 4.84

Chi-Square for Independence Model with 66 Degrees of Freedom = 1296.53
Independence AIC = 1320.53
Model AIC = 128.82
Saturated AIC = 156.00
Independence CAIC = 1375.89
Model CAIC = 253.38
Saturated CAIC = 515.82

Normed Fit Index (NFI) = 0.94
Non-Normed Fit Index (NNFI) = 0.97
Parsimony Normed Fit Index (PNFI) = 0.73
Comparative Fit Index (CFI) = 0.98
Incremental Fit Index (IFI) = 0.98
Relative Fit Index (RFI) = 0.93

Critical N (CN) = 283.36

Root Mean Square Residual (RMR) = 0.052
Standardized RMR = 0.052
Goodness of Fit Index (GFI) = 0.98
Adjusted Goodness of Fit Index (AGFI) = 0.97
Parsimony Goodness of Fit Index (PGFI) = 0.64

Fitted Covariance Matrix

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT	Gtrust
IMPCErr	1.00					
IMPCCol	0.48	1.00				
IMPCIA	0.63	0.62	1.00			
IMPCUSU	0.57	0.56	0.73	1.00		
OWDSenT	-0.12	-0.25	-0.15	-0.14	1.00	
Gtrust	0.09	0.09	0.11	0.10	-0.02	1.00
GSDCon	-0.02	-0.02	-0.03	-0.03	0.01	-0.12
GSDHon	0.06	0.06	0.08	0.07	-0.02	0.31
LOCIntr	0.04	0.04	0.05	0.05	-0.01	0.21
LOCPOr	-0.06	-0.06	-0.08	-0.07	0.01	-0.31
LOCChar	-0.07	-0.07	-0.09	-0.08	0.02	-0.36
RiskPro	-0.04	-0.03	-0.05	-0.04	0.01	-0.18

Fitted Covariance Matrix

	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskPro
GSDCon	1.00					
GSDHon	-0.09	1.00				
LOCIntr	-0.06	0.15	1.00			
LOCPOr	0.08	-0.22	-0.15	1.00		
LOCChar	0.10	-0.26	-0.17	0.64	1.00	
RiskPro	0.05	-0.13	-0.09	0.12	0.14	1.00

Fitted Residuals

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT	Gtrust
IMPCErr	0.00					
IMPCCol	0.02	0.00				
IMPCIA	-0.02	-0.03	0.00			
IMPCUSU	-0.08	-0.04	-0.02	0.00		
OWDSenT	-0.03	0.00	0.00	-0.01	0.00	
Gtrust	-0.07	-0.10	-0.07	-0.02	0.10	0.00
GSDCon	0.09	0.00	0.06	-0.01	0.00	0.05
GSDHon	0.04	-0.08	-0.03	0.03	-0.06	-0.09
LOCIntr	0.04	0.03	-0.01	0.01	0.02	-0.02
LOCPOr	-0.02	0.03	0.02	0.00	0.05	0.05
LOCChar	0.03	0.02	0.02	-0.07	0.03	0.05
RiskPro	-0.08	-0.05	-0.09	-0.08	0.01	-0.06

Fitted Residuals

	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskPro
GSDCon	0.00					
GSDHon	0.01	0.00				
LOCIntr	0.05	0.07	0.00			
LOCPOr	0.09	-0.01	0.14	0.00		
LOCChar	0.04	-0.03	0.06	-0.02	0.00	
RiskPro	-0.01	0.12	0.06	-0.14	-0.08	0.00

Summary Statistics for Fitted Residuals

```
Smallest Fitted Residual =   -0.14
  Median Fitted Residual =    0.00
 Largest Fitted Residual =    0.14
```

Stemleaf Plot

```
- 1|40
- 0|9988888777665
- 0|433332222221111100000000000000000
  0|1112222233333444
  0|55555666799
  1|024
```

Standardized Residuals

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT	Gtrust
IMPCErr	- -					
IMPCCol	0.87	- -				
IMPCIA	-1.72	-2.37	- -			
IMPCUSU	-3.13	-1.94	-1.96	- -		
OWDSenT	-0.69	0.22	0.18	-0.46	- -	
Gtrust	-1.34	-1.96	-1.83	-0.37	1.77	- -
GSDCon	1.61	0.07	0.96	-0.19	0.07	1.45
GSDHon	0.67	-1.49	-0.57	0.55	-1.06	-3.34
LOCIntr	0.73	0.49	-0.25	0.26	0.29	-0.71
LOCPOr	-0.29	0.57	0.48	0.01	0.83	1.85
LOCChar	0.50	0.40	0.34	-1.42	0.54	2.31
RiskPro	-1.32	-0.90	-1.66	-1.34	0.20	-2.16

Standardized Residuals

	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar	RiskPro
GSDCon	- -					
GSDHon	0.28	- -				
LOCIntr	0.94	1.75	- -			
LOCPOr	1.91	-0.20	3.01	- -		
LOCChar	0.95	-0.96	1.47	-2.09	- -	
RiskPro	-0.20	2.51	1.07	-2.91	-1.76	- -

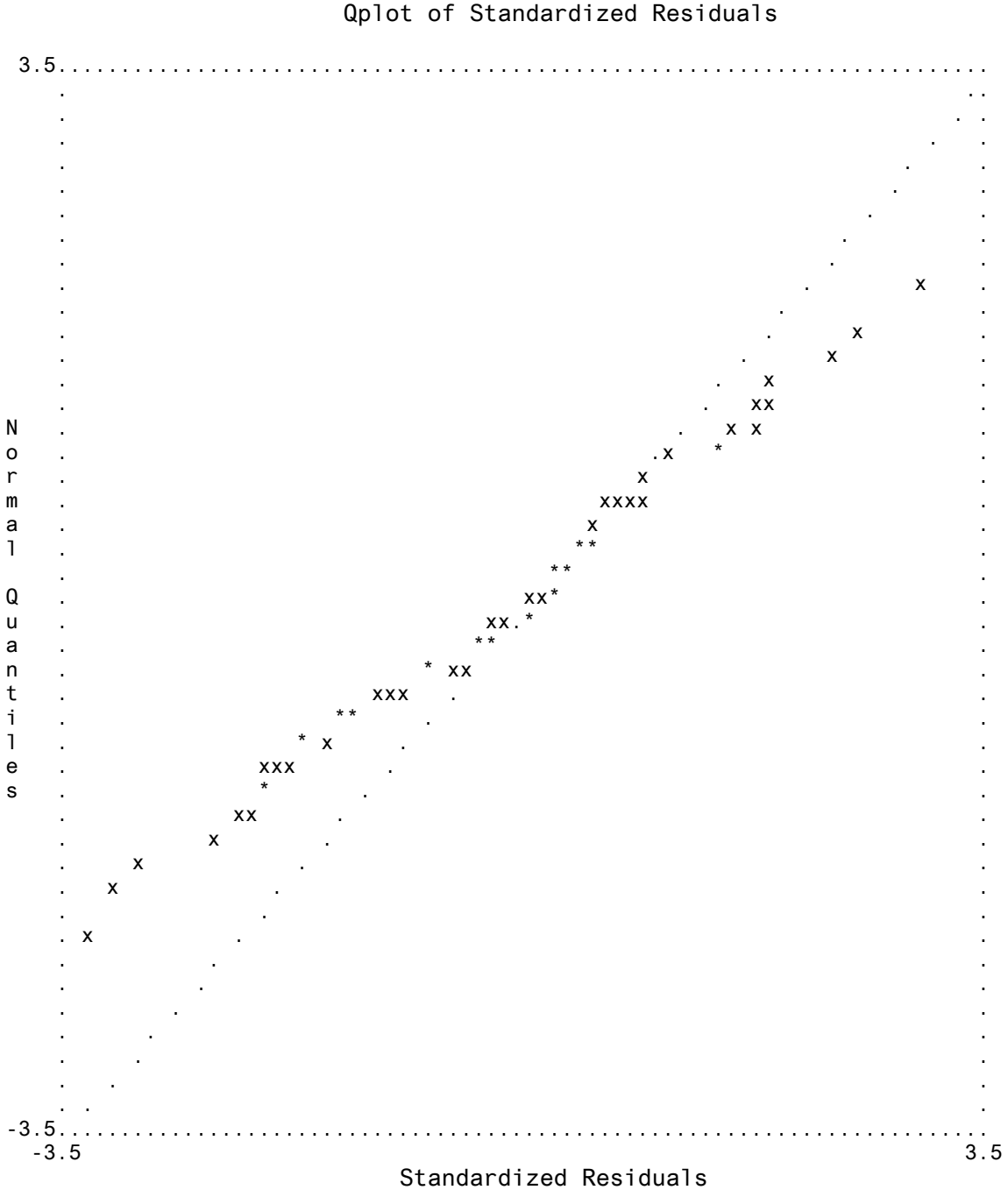
Summary Statistics for Standardized Residuals

```
Smallest Standardized Residual =   -3.34
  Median Standardized Residual =    0.00
 Largest Standardized Residual =    3.01
```

```
Stemleaf Plot

 - 3|31
 - 2|942100
 - 1|988775433310
 - 0|977654322220000000000000
   0|112223333455556677899
   1|0014567889
   2|35
   3|0

Largest Negative Standardized Residuals
 Residual for  IMPCUSU and  IMPCErr  -3.13
 Residual for   GSDHon and   Gtrust  -3.34
 Residual for  RiskPro and   LOCPOr  -2.91
 Largest Positive Standardized Residuals
 Residual for   LOCPOr and  LOCIntr   3.01
```



Modification Indices and Expected Change
No Non-Zero Modification Indices for LAMBDA-Y
No Non-Zero Modification Indices for LAMBDA-X
No Non-Zero Modification Indices for BETA
No Non-Zero Modification Indices for GAMMA
No Non-Zero Modification Indices for PHI
No Non-Zero Modification Indices for PSI

Modification Indices for THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
IMPCErr	- -				
IMPCCol	4.49	- -			
IMPCIA	0.05	1.70	- -		
IMPCUSU	4.00	0.02	4.11	- -	
OWDSenT	0.00	- -	0.26	0.33	- -

Expected Change for THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
IMPCErr	- -				
IMPCCol	0.09	- -			
IMPCIA	0.01	-0.05	- -		
IMPCUSU	-0.08	-0.01	0.13	- -	
OWDSenT	0.00	- -	0.02	-0.02	- -

Completely Standardized Expected Change for THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
IMPCErr	- -				
IMPCCol	0.09	- -			
IMPCIA	0.01	-0.05	- -		
IMPCUSU	-0.08	-0.01	0.13	- -	
OWDSenT	0.00	- -	0.02	-0.02	- -

Modification Indices for THETA-DELTA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
Gtrust	0.60	0.40	0.74	0.64	3.64
GSDCon	3.49	1.12	0.77	0.98	0.14
GSDHon	2.63	5.45	0.12	0.67	2.15
LOCIntr	0.66	1.34	0.36	0.01	0.17
LOCPOr	3.35	0.16	0.16	1.37	0.86
LOCChar	1.59	0.17	0.38	2.82	0.01
RiskPro	1.85	0.08	0.73	0.00	0.98

Expected Change for THETA-DELTA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
Gtrust	-0.03	-0.03	-0.03	0.03	0.10
GSDCon	0.08	-0.05	0.03	-0.04	-0.02
GSDHon	0.07	-0.10	-0.01	0.03	-0.08
LOCIntr	0.04	0.05	-0.02	0.00	0.02
LOCPOr	-0.06	0.01	-0.01	0.04	0.04
LOCChar	0.04	-0.01	0.02	-0.05	0.00
RiskPro	-0.06	0.01	-0.03	0.00	0.05

Completely Standardized Expected Change for THETA-DELTA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
Gtrust	-0.03	-0.03	-0.03	0.03	0.10
GSDCon	0.08	-0.05	0.03	-0.04	-0.02
GSDHon	0.07	-0.10	-0.01	0.03	-0.08
LOCIntr	0.04	0.05	-0.02	0.00	0.02
LOCPOr	-0.06	0.01	-0.01	0.04	0.04
LOCChar	0.04	-0.01	0.02	-0.05	0.00
RiskPro	-0.06	0.01	-0.03	0.00	0.05

Modification Indices for THETA-DELTA

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	- -					
GSDCon	2.80	- -				
GSDHon	3.58	0.02	- -			
LOCIntr	0.94	0.01	5.48	- -		
LOCPOr	4.09	4.59	0.00	6.77	- -	
LOCChar	1.45	0.21	0.94	0.09	- -	- -
RiskPro	13.37	1.10	2.91	1.87	7.39	0.20

Modification Indices for THETA-DELTA

	RiskPro
RiskPro	- -

Expected Change for THETA-DELTA

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	- -					
GSDCon	0.10	- -				
GSDHon	-0.15	-0.01	- -			
LOCIntr	0.07	0.00	0.14	- -		
LOCPOr	-0.12	0.10	0.00	0.12	- -	
LOCChar	0.07	-0.02	-0.05	-0.01	- -	- -
RiskPro	-0.26	0.06	0.09	0.08	-0.12	0.02

Expected Change for THETA-DELTA

	RiskPro
RiskPro	- -

Completely Standardized Expected Change for THETA-DELTA

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	- -					
GSDCon	0.10	- -				
GSDHon	-0.15	-0.01	- -			
LOCIntr	0.07	0.00	0.14	- -		
LOCPOr	-0.12	0.10	0.00	0.12	- -	
LOCChar	0.07	-0.02	-0.05	-0.01	- -	- -
RiskPro	-0.26	0.06	0.09	0.08	-0.12	0.02

Completely Standardized Expected Change for THETA-DELTA

	RiskPro
RiskPro	- -

Maximum Modification Index is 13.37 for Element (7, 1) of THETA-DELTA

Standardized Solution

LAMBDA-Y

	OnLinePO
IMPCErr	0.70
IMPCCol	0.69
IMPCIA	0.90
IMPCUSU	0.81
OWDSenT	-0.17

LAMBDA-X

	FunPriOr
Gtrust	0.66
GSDCon	-0.18
GSDHon	0.47
LOCIntr	0.32
LOCPOr	-0.46
LOCChar	-0.54
RiskPro	-0.26

GAMMA

	FunPriOr
OnLinePO	0.19

Correlation Matrix of ETA and KSI

	OnLinePO	FunPriOr
OnLinePO	1.00	
FunPriOr	0.19	1.00

PSI

	OnLinePO
	0.96

Regression Matrix ETA on KSI (Standardized)

	FunPriOr
OnLinePO	0.19

Completely Standardized Solution

LAMBDA-Y

	OnLinePO
IMPCErr	0.70
IMPCCol	0.69
IMPCIA	0.90
IMPCUSU	0.81
OWDSenT	-0.17

LAMBDA-X

	FunPriOr
Gtrust	0.66
GSDCon	-0.18
GSDHon	0.47
LOCIntr	0.32
LOCPOr	-0.46
LOCChar	-0.54
RiskPro	-0.26

GAMMA

	FunPriOr
OnLinePO	0.19

Correlation Matrix of ETA and KSI

	OnLinePO	FunPriOr
OnLinePO	1.00	
FunPriOr	0.19	1.00

PSI

	OnLinePO
	0.96

THETA-EPS

	IMPCErr	IMPCCol	IMPCIA	IMPCUSU	OWDSenT
IMPCErr	0.51				
IMPCCol	- -	0.53			
IMPCIA	- -	- -	0.19		
IMPCUSU	- -	- -	- -	0.34	
OWDSenT	- -	-0.14	- -	- -	0.97

THETA-DELTA

	Gtrust	GSDCon	GSDHon	LOCIntr	LOCPOr	LOCChar
Gtrust	0.56					
GSDCon	- -	0.97				
GSDHon	- -	- -	0.78			
LOCIntr	- -	- -	- -	0.90		
LOCPOr	- -	- -	- -	- -	0.79	
LOCChar	- -	- -	- -	- -	0.39	0.71
RiskPro	- -	- -	- -	- -	- -	- -

THETA-DELTA

	RiskPro
RiskPro	0.93

Regression Matrix ETA on KSI (Standardized)

	FunPriOr
OnLinePO	0.19

Total and Indirect Effects

Total Effects of KSI on ETA

	FunPriOr
OnLinePO	0.19
	(0.08)
	2.51

Total Effects of ETA on Y

	OnLinePO
IMPCErr	0.70
IMPCCol	0.69
	(0.05)
	14.73
IMPCIA	0.90
	(0.05)
	17.23
IMPCUSU	0.81
	(0.05)
	17.41
OWDSenT	-0.17
	(0.06)
	-2.78

Total Effects of KSI on Y

	FunPriOr
IMPCErr	0.13
	(0.05)
	2.51
IMPCCol	0.13
	(0.05)
	2.53
IMPCIA	0.17
	(0.07)
	2.54
IMPCUSU	0.15
	(0.06)
	2.52
OWDSenT	-0.03
	(0.02)
	-1.88

Standardized Total and Indirect Effects

Standardized Total Effects of KSI on ETA

	FunPriOr
OnLinePO	0.19

Standardized Total Effects of ETA on Y

	OnLinePO
IMPCErr	0.70
IMPCCol	0.69
IMPCIA	0.90
IMPCUSU	0.81
OWDSenT	-0.17

Completely Standardized Total Effects of ETA on Y

	OnLinePO
IMPCErr	0.70
IMPCCol	0.69
IMPCIA	0.90
IMPCUSU	0.81
OWDSenT	-0.17

Standardized Total Effects of KSI on Y

	FunPriOr
IMPCErr	0.13
IMPCCol	0.13
IMPCIA	0.17
IMPCUSU	0.15
OWDSenT	-0.03

Completely Standardized Total Effects of KSI on Y

	FunPriOr
IMPCErr	0.13
IMPCCol	0.13
IMPCIA	0.17
IMPCUSU	0.15
OWDSenT	-0.03

Time used: 0.156 Seconds

APPENDIX C

INSTITUTIONAL APPROVAL LETTERS

DENISON INDEPENDENT SCHOOL DISTRICT
B. McDANIEL MIDDLE SCHOOL 400 LILLIS LANE DENISON, TEXAS 75020-3604

OFFICE OF PRINCIPAL

To: Brian Grams
1202 Woodlawn Blvd.
Denison, TX 75020

From: Mr. Alvis Dunlap
B. McDaniel Middle School
400 N Lillis Lane
Denison, TX 75020

Brian,

I have reviewed the information you provided regarding your research entitled *An Empirical Analysis of Factors Influencing Individual Privacy Concerns*. I understand that you are requesting access to our facility, faculty and staff for the purpose of participation in an anonymous survey. I see no issues in allowing you to do so. The administration at B. McDaniel Middle School gives you permission to proceed with the collection of data using your survey. As previously stated only faculty and staff over the age of 18 will be allowed to participate. You may not approach any students for the purposes of collecting data.

If there are any questions or issues regarding this permission I may be contacted at 903-468-7600 weekdays during regular business hours.

Sincerely,

Alvis Dunlap
Principal

A New Dimension In Learning

November 6, 2003

Brian Grams
1202 Woodlawn Blvd
Denison, TX 75020

Dear Brian:

I have reviewed the information you provided regarding your research entitled *An Empirical Analysis of Factors Influencing Individual Privacy Concerns*. I understand that you are requesting access to our facility, faculty, staff, and students for the purpose of participation in an anonymous survey. I see no issues in allowing you to do so. The administration of Grayson County College gives you permission to proceed with the collection of data using your survey. Faculty, staff and students over the age of 18 will be allowed to participate. You may not collect data from any students under the age of 18 for the purpose of your study.

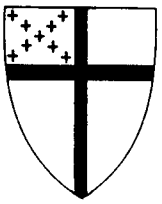
If there are any questions or issues regarding this permission I may be contacted at 903-463-8600 weekdays during regular business hours.

Sincerely,

Alan Scheibmeir

Alan Scheibmeir, Ph.D.
President

Grayson County College
Sherman - Denison
6101 Grayson Drive • Denison, Texas 75020-8299
(903) 465-6030 FAX (903) 463-5284



St. Luke's School

January 26, 2004

Brian Grams
1202 Woodlawn Blvd.
Denison, TX 75020

Dear Mr. Grams:

I have reviewed the information you provided regarding your research entitled *An Empirical Analysis of Factors Influencing Individual Privacy Concerns.* I understand that you are requesting access to our facility, faculty, and staff for the purpose of participation in an anonymous survey. I see no issues in allowing you to do so. The administration of St. Luke's Episcopal School gives you permission to proceed with the collection of data using your survey. Faculty and staff will be allowed to participate.

If there are any questions or issues regarding permission, I may be contacted at (903) 465-2653 weekdays during regular school hours.

Sincerely,

Karen Wilson

Karen Wilson
Headmistress

427 W. WOODARD • DENISON, TEXAS 75020 • (903) 465-2653

APPENDIX D

APPROVALS AND CERTIFICATES: RESEARCH INVOLVING HUMAN SUBJECTS

UNIVERSITY of NORTH TEXAS

Office of Research Services

November 24, 2003

Brian Grams
School of Library and Information Sciences
University of North Texas

RE: Human Subjects Application No. 03-343

Dear Mr. Grams,

Your proposal titled "An Empirical Analysis of Factors Influencing Individual Privacy Concerns" has been approved by the Institutional Review Board and is exempt from further review under 45 CFR 46.101. **Federal policy 45 CFR 46.109(e) stipulates that IRB approval is for one year only.**

Enclosed is the consent document with stamped IRB approval. Please copy and **use this form only** for your study subjects.

U.S. Department of Health and Human Services regulations require that you submit annual and terminal progress reports to the UNT Institutional Review Board. Further, the UNT IRB must re-review this project annually and/or prior to any modifications you make in the approved project. Please contact me if you wish to make such changes or need additional information.

Sincerely,

Scott Simpkins, Ph.D.
Chair
Institutional Review Board

SS:sb

P.O. Box 305250 • Denton, Texas 76203-5250 • (940) 565-3940
Fax (940) 565-4277 • TTY (800) RELAY TX • www.unt.edu

UNIVERSITY of NORTH TEXAS

Office of Research Services

February 4, 2004

Brian Grams
School of Library and Information Sciences
University of North Texas

Institutional Review Board for the Protection of Human Subjects in Research (IRB)
RE: Human Subject Application #03-343

Dear Mr. Grams,

The UNT IRB has received your request to modify your study titled "An Empirical Analysis of Factors Influencing Individual Privacy Concerns." As required by federal law and regulations governing the use of human subjects in research projects, the UNT IRB has examined the requested changes. The modification to this study is hereby approved for the use of human subjects. **Approval for this project is November 24, 2003 through November 23, 2004.**

It is your responsibility according to U.S. Department of Health and Human Services regulations to submit annual and terminal progress reports to the IRB for this project. Please mark your calendar accordingly. The IRB must also review this project prior to any other modifications made. **Federal policy 21 CFR 56.109(e) stipulates that IRB approval is for one year only.**

Please contact Shelia Bourns, Compliance Administrator, at (940) 565-3940,or Boyd Herndon, Assistant Director for Compliance, at (940) 565-3941, if you wish to make changes or need additional information.

Sincerely,

Scott Simpkins, Ph.D.
Chair
Institutional Review Board

SS/sb

P.O. Box 305250 • Denton, Texas 76203-5250 • (940) 565-3940
Fax (940) 565-4277 • TTY (800) RELAY TX • www.unt.edu

You must be a minimum of 18 years old to participate in this study.

University of North Texas
Institutional Review Board
Research Project Information Sheet

Title of Study: An empirical analysis of factors influencing individual privacy concerns

Principal Investigator: Brian Grams, student, University of North Texas

Co-Investigator: Linda Schamber, Ph.D., faculty advisor, University of North Texas School of Library and Information Sciences

Before agreeing to participate in this research study, it is important that you read and understand the following explanation of the proposed research method. It describes the procedures, benefits, and any potential risks of the study. It also describes your rights as an individual to withdraw from the study at any time. It is important for you to understand that no guarantees or assurances are implied or associated with the results of this study.

Purpose of the Study: The study seeks to gather information about individuals' opinions concerning privacy and behavior related to privacy.

Description of the Study: The study will use a survey consisting of questions and statements designed to collect information about individuals' attitudes toward privacy.

Procedures to be used: An anonymous survey, which takes approximately 25 minutes to complete, will be used to collect information regarding the attitudes and opinions of adults over 18 years of age.

Description of the foreseeable risks: None

Benefits to the participants or others: This study is intended to contribute to a better understanding of individuals' attitudes related to privacy. This study and the resulting analysis are intended to contribute to the development of privacy related policy and technologies that will benefit both individuals and organizations.

Procedures for Maintaining Confidentiality of Research Records: All data collection will be performed using a survey that has no means of participant identification anywhere on the instrument.

Review for the Protection of Participants
This study has been approved by the University of North Texas Institutional Review Board (IRB). If you have any questions about your rights as a research participant you may contact the UNT IRB at (940) 565-3940.

Research Participant's Rights
I have read or have had read to me all of the above. Brian Grams has offered to explain the study to me and answer my questions. I have been informed of any risks as well as the possible benefits of the study. I understand that my refusal to participate, or my decision to withdraw will involve no penalty or loss of rights, benefits, or legal recourse to which I am entitled. The study personnel may choose to stop my participation at any time. In case problems or questions arise about the research project, I have been told I can contact Brian Grams by telephone at 903-465-4565 or email him at bcg0011@unt.edu, or alternatively contact Linda Schamber, Ph.D., faculty advisor, at 940-565-3568, for clarification or answers. I understand my rights as a research participant, and by participating I confirm I am an adult at least 18 years old and I voluntarily consent to take part in this study.

APPROVED BY THE UNT IRB
FROM 11/24/03 TO 11/23/04

Please keep this information sheet for your reference.

Completion Certificate

This is to certify that

Brian Grams

has completed the **Human Participants Protection Education for Research Teams** online course, sponsored by the National Institutes of Health (NIH), on 01/28/2003.

This course included the following:

- key historical events and current issues that impact guidelines and legislation on human participant protection in research.
- ethical principles and guidelines that should assist in resolving the ethical issues inherent in the conduct of research with human participants.
- the use of key ethical principles and federal regulations to protect human participants at various stages in the research process.
- a description of guidelines for the protection of special populations in research.
- a definition of informed consent and components necessary for a valid consent.
- a description of the role of the IRB in the research process.
- the roles, responsibilities, and interactions of federal agencies, institutions, and researchers in conducting research with human participants.

National Institutes of Health
http://www.nih.gov

APPENDIX E

SAMPLE SOLICITATION LETTER

Fellow faculty and staff,

My husband, Brian, is currently working on a research project in conjunction with his course work at the University of North Texas. He is looking for volunteers to fill out a survey that takes about 25 minutes and deals with the subject of privacy and personal information. You might find the survey interesting. You may find that it provokes a measure of self-reflection on how you feel about yourself and some things that affect you in the world today.

Recognizing the fact that everyone's time is valuable, those that participate in the survey will be able to enter a drawing for a prize. The individual whose name is drawn from the entries will receive a $25.00 gift certificate to Chili's restaurant. There will be a random drawing soon after the conclusion of the study at B. McDaniel. If you agree to participate, instructions for entering the drawing will be included with the survey package you receive.

If you would like to participate in this study, please mark the box in the space provided at the bottom of the sheet and return it to Janice Grams' school mailbox before 12/08/03. A spouse not employed at B. McDaniel Middle School may also enter the drawing for the gift certificate. The only requirement is the spouse's willingness to participate in the study by completing a survey. If you decide to participate, on or about January 7, 2004, you will receive a survey packet in your school mailbox containing the survey(s), research project information sheet(s), drawing entry form(s), and instructions for returning the survey(s) when you have finished.

We appreciate your time and consideration.

Janice Grams
&
Brian Gram

Mark the box if you would like to participate in the survey: ☐

(Print your spouse's name on this line if they would like to participate.)

_____

APPENDIX F

RESULTS OF PILOT STUDY AND PILOT SURVEY

PILOT STUDY EVALUATION

This appendix outlines the pilot study that was performed and the changes that resulted as a consequence of the findings. Descriptive statistics resulting from the study are provided. As a result of the pilot several changes were made to the survey instrument. The pilot survey prior to the changes is located in at the end of this appendix. The final survey is located in Appendix A if the reader would like to make a comparison of the instruments.

The Sample

An initial pilot study was conducted at B. McDaniel Middle School in Denison, Texas. Potential participants consisted of faculty and staff. Institutional permission was granted (see Appendix A) and individual participants were solicited using a letter that was delivered to each individual's institutional mail box (see Appendix B). The letter also encouraged participant's spouses and friends to participate in the study. A drawing for a prize, consisting of a gift certificate to a local restaurant, was offered as an incentive for individuals to participate in the study. There were 102 letters distributed, and a total of 58 individuals volunteered to participate in the pilot study.

Survey Response: Problems

All 58 volunteers returned the survey in various states of completion. A number of issues related to response patterns invalidated 16, or more than 27% of the 58 returned surveys. The resulting 42 completed surveys were used for a preliminary analysis.

Of the 16 surveys deemed invalid, three individuals left the first section of the survey dealing with self-evaluation of personality characteristics completely blank.

These individuals filled out the second and third sections related to privacy perceptions and demographics. It would appear these individuals did not feel comfortable evaluating or disclosing information about their personality. Another six individuals chose to complete the section requesting a self-report of online disclosure with checkmarks instead of the true/false response requested in the instructions. One participant who completed the section in this manner made the comment it was easier just to check the appropriate items. This rendered the responses invalid. Seven other individuals either skipped or chose not to answer various questions throughout the survey and were also eliminated before analyzing the results. While various statistical methods could be employed to compensate for some of the missing data it was not deemed appropriate for a preliminary analysis of pilot data.

Several problems became apparent while reviewing the responses with respect to flow and means of response. As a result of these issues the original survey (see Appendix C) has been modified to improve flow, clarify instructions, or improve the method of response such that there will be a higher probability of valid participant responses. The final version of the survey instrument is contained in Appendix D.

Survey Instrument Changes: Summary

The modifications and additions being described were made to the initial survey to address a number of response problems and improve flow on a number of items. The majority of the modifications were in response to the surveys that had to be discarded due to unacceptable responses or lack of responses. Some changes were made to improve other aspects of usability. Each will be described in detail.

In reviewing the instrument used to evaluate trust it was discovered that an item relevant to the study had been omitted. The item that was contained in the original instrument related to the participants perception of the disclosiveness of others. The item, confidential/divulging, was added to the scale and complimented with an equivalent item secretive/talkative.

The portion of the survey related to online disclosure was significantly modified. In the pilot study this portion of the survey resulted in the most consistent response failure that resulted in discarding the entire observation. As mentioned previously, six of the respondents simply checked appropriate items related to their last online experience instead of providing the requested true or false reply. In order to eliminate this problem in the future, check boxes for a T/F response were added. In addition, instruction/flow for the first item was modified such that if the respondent had never made online disclosures of personal information they were not required to read through the instructions before moving to the next section.

Initially four items had been included with the intention of determining some type of weighting mechanism for the response to the online disclosure section. After further review it could not be established that there was a substantial theoretical foundation for such an approach. As a consequence four items that were intended for this purpose were eliminated.

In this online disclosure section the disclosure target language was modified to improve uniformity. The original items had mixed references to a Web site and a company interspersed throughout the items. The language was modified so that

references to a company were altered to be consistent with Web site references. Instructions were tailored to reflect all of the above modifications to this section.

Based on an analysis of responses in the section addressing online willingness to disclose it was apparent that the initial section requesting a method of contact was redundant with the personal contact section of the instrument. As a result I deleted the section requesting addresses at the top of the page and added the email item to the contact section. The original instrument initially instructed the participant to write a T or F in a blank, or to leave the item blank if it did not apply to them, To simplify and clarify the means of response I provided check boxes for a yes (Y), no (N) or not applicable (N/A) response. Instructions were also inserted where appropriate to skip sections if dictated by the participants' circumstances, such as not having children or not being married. Instrument instructions were modified to reflect all of the changes.

The last modification made was to the first two items in the demographic section dealing with the computer and online experience of the participant. Statement patterns were modified to improve item flow and jumps.

Demographics

In the pilot study, participants completing the demographics consisted of 38 females and 16 males with an average age of 44. Eight-five percent had at least a bachelor's degree, and 68% had annual incomes in the range of $25,000 to $50,000. Eighteen percent indicated they had been the victim of credit card fraud, checking fraud, or identity theft and 36% indicated that they had had their personal information used improperly by a company. Outside of a high ratio of females, the sample appeared to be relatively homogenous.

Privacy & Personal Information: A Survey

This survey is intended to explore some of the ways people feel about themselves and other people, and how they relate to the world around them. It is administered anonymously in the hope that those willing to participate will feel comfortable responding to all of the items without concern for things that might otherwise make them uncomfortable, such as sharing personal information with someone they don't know. *Please make sure you do not sign your name or place any other kind of identifying mark on the survey.* The survey should take around 25 minutes to complete.

There are no right or wrong answers. Answers can only be compared to the answers of others that have completed this survey or one similar. Replies cannot be compared to any type of index or scale that would indicate anything more, such as would be the case with something like an IQ test.

Please don't try to second-guess yourself. Generally the first response that you give is the closest to how you actually feel about something, and how you feel is what this is all about.

Different methods or scales are used on the survey to indicate your views, perspectives, or feelings about the statements. There are specific instructions for various portions of the survey. There are some general questions about you at the end of the survey. I appreciate your willingness to share your feelings, your candidness, and your honesty. If you have any questions please feel free to ask. You may contact me as indicated on the Research Project Information Sheet that was included in your survey package.

Thank you very much.

Brian Grams

Instructions: Read each statement carefully. Circle the number on the scale that is the closest description of the way you feel about the statement. First impressions are usually best. Please be sure to respond to every statement. If the numbers used for answers do not adequately reflect your own opinion, use the one that is closest to the way you feel.

1. I'm very careful when I make plans and when I act on them.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
2. I follow the motto, 'nothing ventured, nothing gained'	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
3. I don't have much sympathy for adventurous decisions.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
4. Quite often I will do things I haven't done before without really thinking about it.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
5. If a task seems interesting I'll choose to do it even if I'm not sure whether I'll be able to manage it.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
6. I don't like to risk things; I would rather be on the safe side.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
7. Even when I know that my chances of success are limited, I will try my luck.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
8. In my work I set goals so that I can achieve them without difficulty.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
9. I express my opinion even if most people have opposite views.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
10. My decisions are always made carefully and accurately.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
11. I would like my boss's job some time so I could show my competence, despite the risk of making mistakes.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
12. I tend to think about the unfavorable outcomes of my actions.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
13. Success encourages me to take bigger risks.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me
14. If I really want to do something, I will go ahead, do it, and worry about the consequences later.	**1** Not at all true for me	**2**	**3**	**4**	**5**	**6**	**7** Very true for me

Some activities involve a "*physical*" risk, such as particular occupations (e.g. fireman, policeman, military) or sports (e.g. rock-climbing, skydiving) or transportation (e.g. cycling) - that is, there is a risk of getting injured in an accident or possibly even being killed.

15. In general, my tendency to accept ***physical*** risks is...

1 Extremely Low — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9 — 10 Extremely High

Some activities involve a "financial" risk, such as starting a business, investing in the stock market, or gambling (e.g. in casinos) and betting (e.g. on horses) - that is, there is a risk of losing money or other assets.

16. In general, my tendency to accept ***financial*** risks is ...

1 Extremely Low — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9 — 10 Extremely High

Some activities involve a "health" risk, such as traveling overseas (e.g. in countries of low hygienic standards) or particular "lifestyle" behaviors (e.g. long sunbathing, unsafe sex, drugs for pleasure) or smoking - that is, there is a risk of catching a harmful disease.

17. In general, my tendency to accept ***health*** risks is ...

1 Extremely Low — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9 — 10 Extremely High

Some activities involve a "*social*" risk, such as being outspoken or behaving in an unusual manner (e.g. openly challenging or disagreeing with commonly accepted views, deviating sexually, or violating social norms) or accepting public roles (e.g. giving an unpopular or controversial speech) - that is, there is a risk of losing the respect and acceptance of others and harming one's social status.

18. In general, my tendency to accept ***social*** risks is ...

1 Extremely Low — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9 — 10 Extremely High

19. Overall, how would you rate your general willingness to take a risk *in comparison to other people*, such as your family, friends, or acquaintances?

1 Extremely Low — 2 — 3 — 4 — 5 — 6 — 7 — 8 — 9 — 10 Extremely High

Instructions: Please mark the following statements to reflect how you communicate with people in general. Indicate the degree to which the following statements reflect how you communicate with people by circling the number on the scale that is the closest to a description of the way you feel about the statement. Please be sure to mark all statements.

1. I do not always feel completely sincere when I reveal my own feelings, emotions, behaviors or experiences.

7 Strongly agree — 6 Agree — 5 Agree somewhat — 4 Undecided — 3 Disagree somewhat — 2 Disagree — 1 Strongly disagree

2. I intimately disclose who I really am, openly and fully in my conversation.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
3. I do not often talk about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
4. Only infrequently do I express my personal beliefs and opinions.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
5. I am not always honest in my self-disclosures.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
6. Once I get started, my self-disclosures last a long time.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
7. I often talk about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
8. I always feel completely sincere when I reveal my own feelings and experiences.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
9. I feel that I sometimes do *not* control my self-disclosure of personal or intimate things I tell about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
10. I am often not confident that my expressions of my own feelings, emotions, and experiences are true reflections of myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
11. My conversation lasts the least time when I am discussing myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
12. My statements about my feelings, emotions, and experiences are always accurate self-perceptions.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
13. I often disclose intimate, personal things about myself without hesitation.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
14. I often discuss my feelings about myself.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree

15. Once I get started, I intimately and fully reveal myself in my self-disclosures.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
16. My self-disclosures are completely accurate reflections of who I really am.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
17. I usually talk about myself for fairly long periods at a time.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
18. I cannot reveal myself when I want to because I do not know myself thoroughly enough.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
19. My statements of my feelings are usually brief.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree
20. I am always honest in my self-disclosures.	**7** Strongly agree	**6** Agree	**5** Agree somewhat	**4** Undecided	**3** Disagree somewhat	**2** Disagree	**1** Strongly disagree

Instructions: The following 24 items are a series of attitude statements. Each represents a commonly held opinion. There are no right or wrong answers. You will probably agree with some items and disagree with others. We are interested in the extent to which you agree or disagree with such matters of opinion.
Read each statement carefully. Then indicate the extent to which you agree or disagree by circling the number on the scale that is the closest description of the way you feel about the statement. First impressions are usually best. Please be sure to respond to every statement. If you find that the numbers used in answering do not adequately reflect your own opinion, use the one that is closest to the way you feel.

	-3	-2	-1	1	2	3
1. Whether or not I get to be a leader depends mostly on my ability.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
2. To a great extent my life is controlled by accidental happenings.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
3. I feel like what happens in my life is mostly determined by powerful people.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
4. Whether or not I get into a car accident depends mostly on how good a driver I am.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
5. When I make plans, I am almost certain to make them work.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
6. Often there is no chance of protecting my personal interests from bad luck happenings.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
7. When I get what I want, it's usually because I'm lucky.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
8. Although I might have good ability, I will not be given leadership responsibility without appealing to those in positions of power.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
9. How many friends I have depends on how nice a person I am.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
10. I have often found that what is going to happen will happen.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree

	-3	-2	-1	1	2	3
11. My life is chiefly controlled by powerful others.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
12. Whether or not I get into a car accident is mostly a matter of luck.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
13. People like myself have very little chance of protecting our personal interests when they conflict with those of strong pressure groups	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
14. It's not always wise for me to plan too far ahead because many things turn out to be a matter of good or bad fortune.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
15. Getting what I want requires pleasing those people above me.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
16. Whether or not I get to be a leader depends on whether I'm lucky enough to be in the right place at the right time.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
17. If important people were to decide they didn't like me, I probably wouldn't make many friends.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
18. I can pretty much determine what will happen in my life.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
19. I am usually able to protect my personal interests.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
20. Whether or not I get into a car accident depends mostly on the other driver.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
21. When I get what I want, it's usually because I worked hard for it.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
22. In order to have my plans work, I make sure that they fit in with the desires of people who have power over me.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree

	-3	-2	-1	1	2	3
23. My life is determined by my own actions.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree
24. It's chiefly a matter of fate whether or not I have a few friends or many friends.	Strongly Disagree	Disagree somewhat	Slightly disagree	Slightly agree	Agree somewhat	Strongly Agree

Instructions: On the scales that follow, please indicate your reaction to people in general. Place a check in the box that represents your immediate feelings about people. Check in the direction of the end of the scale that seems to be the most characteristic of the people you deal with on a daily basis. Place only one check on each line and please mark all lines.

I feel that most people are:

Trustworthy	☐	☐	☐	☐	☐	☐	☐	Untrustworthy
Exploitive	☐	☐	☐	☐	☐	☐	☐	Benevolent
Safe	☐	☐	☐	☐	☐	☐	☐	Dangerous
Deceptive	☐	☐	☐	☐	☐	☐	☐	Candid
Not deceitful	☐	☐	☐	☐	☐	☐	☐	Deceitful
Tricky	☐	☐	☐	☐	☐	☐	☐	Straightforward
Respectful	☐	☐	☐	☐	☐	☐	☐	Disrespectful
Inconsiderate	☐	☐	☐	☐	☐	☐	☐	Considerate
Honest	☐	☐	☐	☐	☐	☐	☐	Dishonest
Unreliable	☐	☐	☐	☐	☐	☐	☐	Reliable
Insincere	☐	☐	☐	☐	☐	☐	☐	Sincere
Careful	☐	☐	☐	☐	☐	☐	☐	Careless

Instructions: Think about the last time you volunteered to give a Web site personal information about yourself to get something in return, such as providing personal information for a purchase or to acquire some other type of benefit from the site. You may or may not have identified yourself, but still provided personal information. Based on your memory of that experience are the following statements about various aspects or impressions of your online experience true (T) or false (F)?

1. ☐ **Mark this box if you have never provided personal information to a company online then move on to the next section.**
2. ____ The company can tell exactly who I am with the information I gave them.
3. ____ This was *not* my first experience at this Web site.
4. ____ This Web site was referred to me by someone I trust.
5. ____ The company requested too much personal information for what they were offering in return.
6. ____ I can't control what the company will do with my information.
7. ____ I provided information that was required to get what I wanted and skipped the rest.
8. ____ The company asked too much personal information so I left the site without finishing.
9. ____ I was asked for some things that made me uncomfortable, but I provided the information anyway.
10. ____ I would recommend the site to my friends and relatives.
11. ____ I provided information that I wouldn't want to give to just anyone.
12. ____ I checked the Web site to see what the company would do with the information before I provided it.
13. ____ All the answers I provided were accurate and honest.
14. ____ I didn't provide all the information that was requested.
15. ____ I made sure the site was secure before I provided any information
16. ____ I would not go back to the site again.
17. ____ I checked the site's privacy policy before giving them any information.

Instructions: The following statements are intended to relate to your feelings about other people who have access to and use of, or otherwise deal with your personal information. Personal information includes, among other things, information about you that can be used to identify you as an individual such as your name, phone number, address, credit card numbers, and Social Security number. Personal information may also include information about you that you wouldn't want the general public to have access to, or know about and be able to associate with you in particular. This type of information may include knowledge such as specific things that have happened to you, things you have participated in such as political activism, or such things as your personal preferences, habits, or behaviors. Using the scale to the right of each statement, indicate your level of agreement with the statement by circling the number on the scale that is the closest description of the way you feel about the statement.

1. It usually bothers me when companies ask me for personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
2. All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
3. Companies should not use personal information for any purpose unless it has been authorized by the individual who provided the original information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
4. Companies should devote more time and effort to preventing unauthorized access to personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
5. When companies ask me for personal information, I sometimes think twice before providing it.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
6. Companies should take more steps to make sure that the personal information in their files is accurate.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
7. Government regulation is the best way to protect my personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
8. When people give personal information to a company for some reason, the company should never use the information for any other reason.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
9. I am comfortable with the ways most companies use my personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
10. Companies should have better procedures to correct errors in personal information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
11. Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
12. It bothers me to give personal information to so many companies.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree

13. Companies should never sell the personal information in their computer databases to other companies.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
14. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
15. I believe that personal information I have provided online is generally used the way I expected.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
16. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
17. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
18. I'm concerned that companies are collecting too much personal information about me.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
19. Consumers have lost all control over how personal information is collected and used by companies.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
20. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
21. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
22. Being able to control my information is more important than protecting my privacy.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
23. I feel that going online jeopardizes my privacy.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree
24. Too many companies have access to my personal information without my consent.	**1** Strongly Agree	**2**	**3**	**4**	**5**	**6**	**7** Strongly Disagree

Situation: A publisher (sports or health magazine, newspaper, world news, etc.) will provide you with a special free premium online version of its publication containing advice, editorials, late-breaking news, and discounts at some of its advertiser's stores. You think the offer is attractive and would like access to the premium content, which will be made available online even if you don't subscribe to the publisher's print publication. All you have to do is agree to share some requested information about you. The information will be collected at the publisher's online Web site with the condition that all requested information **must** be provided in order to access the premium content.

Instructions: In order to receive the premium services you must provide your name and either an email address or your home mailing address for contact purposes. You may provide both addresses if you wish to do so.
Indicate with a check which of the following you would be willing to provide.

____ Home mailing address ____ Email address

The following is a list of information items a publisher **could** request. You have decided that you really want access to the free premium content being offered. Place a **Y for yes** next to each information item **you would be willing to provide**. Place an **N for no** if you would not be willing to provide that piece of information. Even if a piece of information seems redundant please indicate your willingness to provide that piece of information. If the information does not apply to you, such as not being married or not having children, leave the item blank.

Contact Information		
____ Your work phone number	____ Full Street address (if you get mail at a P. O. Box)	____ Full mailing address
____ Your full name	____ City of residence	____ State of residence
____ Your cell phone number	____ Home phone number	____ Zip code
Likes/Dislikes		
____ Favorite food	____ Favorite TV show	____ Favorite hobby
____ Favorite book	____ Favorite recording artist	____ Favorite movie
____ Favorite magazine	____ Favorite political party	____ Favorite sport team
Spouse's Information		
____ Spouse's weight	____ Spouse's height	____ Spouse's birthday
____ Number of people in household	____ Spouse's date of birth	____ Married on what date
Children's Information		
____ Number of children	____ Children's gender	____ Children's ages
____ School children attend	____ Children's names	

Personal Information

____ Your citizenship	____ Own or rent residence	____ Your date of birth
____ Mother's maiden name	____ Your ethnicity	____ Religious preference
____ Marital status	____ State you were born in	____ Your gender
____ Your education (number of years)	____ If homeowner – value of residence	____ Number of credit cards you own

Medical Information

____ Personal physician's name	____ Date of your last illness/injury	____ Your handicaps
____ Prescribed medications	____ Over the counter medications	____ Your blood type
____ Nature of last illness/injury	____ Your weight	____ Your height

Identification

____ Your driver's license number	____ Your social security number	____ Your employer or student ID number

Employment Information

____ Your occupation	____ Your income	____ If employed, how long in your current job
____ Household income	____ Your employer	

Instructions: The following information that we are asking you to provide will help us understand you a little better. Please check the answer that best describes your activities or habits, or provide the appropriate answer in the space provided.

(check one only)

1. ___ I own or have access to a computer

   ___ I use a computer for online access to the Internet/World Wide Web

   (If you did not check either of the above answers please skip to question 7)

   (check one only)

2. ___ I use my own computer most of the time for online access

   ___ I use someone else's computer most of the time for online access (such as those available in a library or school)

3. I have been using a computer to get online:
   ___ less than a year
   ___ 1 to 3 years
   ___ over 3 years

4. I have been using a computer:
   ___ less than a year
   ___ 1 to 5 years
   ___ over 6 years

5. I get on the Web to do things other than check email or play interactive games:
   ___ several hours every day
   ___ every day
   ___ a few times a week
   ___ not very often

6. On average I purchase things online:
   ___ every month
   ___ every couple of months
   ___ hardly ever
   ___ never

7. I am a: ___ Female ___ Male

8. I was born in the year: 19 _____

9. I am married: ____ Yes ____ No

10. I take care of _____ dependent children in my home.

11. I live with my family or someone else other than a spouse who provides support.
___ Yes
___ No

12. My ethnicity is:
___ White
___ African-American
___ Hispanic
___ Asian/Pacific Islander
___ American Indian/Alaskan Native
___ Nonresident Alien
___ Mixed
___ Unknown

13. My level of education is: **(Please check only the highest level you have completed)**
___ High-school diploma or equivalent
___ Licensed or certified skill not requiring a 4 year degree
___ Some college
___ Bachelor's degree
___ Graduate degree

14. My employment status is:
___ Full-time
___ Part-time
___ Not currently employed, not looking for a job
___ Not currently employed, looking for a job

15. My annual income range is:
___ Less than $15,000
___ $15,000 to $25,000
___ $25,000 to $35,000
___ $35,000 - $50,000
___ $50,000 - $75,000
___ $75,000 or more

16. Have you ever had information about you used illegally such as with credit card or checking fraud, or identity theft?
___ Yes
___ No

17. Are you aware if any company has ever used your personal information without your permission in a way you didn't like?
___ Yes
___ No

18. If you would like, make any comments or offer any suggestions you might have about this survey. Continue on the remaining blank pages if you would like to use more space.

REFERENCES

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. *1st ACM Conference on Electronic Commerce* (pp. 1-8). New York: ACM Press.

Annacker, D., Spiekermann, S., & Strobel, M. (2001). E-privacy: Evaluating a new search cost in online environments. Retrieved March 1, 2005 from sfb.wiwi.hu-berlin.de/papers/2001/dpsfb200180.ps.Z.

Archer, R. L. (1987). Commentary: Self-disclosure, a very useful behavior. In V. J. Derlega, & J. H. Berg (Eds.), *Self-disclosure: theory, research, and therapy* (pp. 329-342). New York: Plenum Press.

Barber, N., & Lanz, J. (2001). Managing the risks of data aggregation. *Bank Accounting & Finance, 14*(2), 7-15.

Baxter, L. A., & Montgomery, B. M. (1996). *Relating: Dialogues and dialectics.* New York: The Guilford Press.

Berg, J. H., & Derlega, V. J. (1987). Themes in the study of self-disclosure. In V. J. Derlega, & J. H. Berg (Eds.), *Self-disclosure: theory, research, and therapy* (pp. 1-7). New York: Plenum Press.

Blanchette, J.-F., & Johnson, D. G. (2002). Data Retention and the panoptic society: The social Benefits of forgetfulness. *The Information Society, 18*(1), 33-45.

Byrne, B. M. (1998). *Structural equation modeling with LISREL, PRELIS, and SIMPLIS: basic concepts, applications, and programming.* Mahwah, NJ: Lawrence Erlbaum Associates.

Cate, F. H. (1997). *Privacy in the information age*. Washington, D.C.: Brookings Institution Press.

Center For Democracy and Technology. (2001, August 29). *Online banking privacy: A slow, confusing start to giving customers control over their information.* Retrieved February 9, 2004 from http://www.cdt.org/privacy/financial/010829onlinebanking.pdf

Chelune, G. J. (1976). Self-disclosure situations survey: A new approach to measuring self-disclosure. *JSAS Catalog of Selected Documents in Psychology, 6*(1), 111-112.

Commission of the European Communities (2001, January). *Unsolicited commercial communications and data protection: Summary of study findings*. Retrieved October 21,2002, from http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf

Cranor, L. F., & LaMacchia, B. A. (1998). Spam. *Communications of the ACM, 41*(8), 74-83.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999, April 14). *Beyond concern: understanding net users' attitudes about online privacy.* Retrieved October 9, 1999, from http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-116.

Culnan, M. J., & Milberg, S. J. (1999, June 14). *Consumer privacy.* Retrieved September 29, 2002 from http://www.gsb.georgetown.edu/dept/facserv/faculty/culnanm/research/conspriv.pdf

Cyber Dialogue. (2001, November 7). *UCO software to address retailers' $6.2 billion privacy problem.* Retrieved September 4, 2002, from http://www.cyberdialogue.com/news/releases/2001/11-07-uco-retail.html

Das, T. K., & Bing-Sheng, T. (2004). The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology, 19*(1), 85-116.

DeCew, J. W. (1997). In pursuit of privacy: law, ethics, and the rise of technology. Ithaca, NY: Cornell University Press.

Derlega, V. J., & Grzelak, J. (1976). Appropriateness of self-disclosure. In G. J. Chelune (Ed.) *Self-disclosure: Origins, patterns, and implication of openness in interpersonal relationships* (pp. 151-176). San Francisco: Jossey-Bass.

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-disclosure*. Newbury Park, CA: Sage Publications.

Electronic Privacy Information Center. (2003, April 28). *Privacy and public records.* Retrieved October 29, 2003, from http://www.epic.org/privacy/publicrecords/default.html

Flaherty, D. H. (1989). *Protecting privacy in surveillance societies*. Chapel Hill, NC: University of North Carolina Press.

Fukuyama, F. (1996). *Trust: The social virtues and the creation of prosperity*. New York: Free Press Paperbacks.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century.* Sebastopol, CA: O'Reilly & Associates.

Griswold v. Connecticut. (1965). 381 U.S. 479.

Hahn, R. W. (2001, May 7). *An assessment of the costs of proposed online privacy legislation.* Association for Competitive Technology. Retrieved March 2, 2005 from http://www.actonline.org/documents/010507Privacystudy.pdf

Harris Interactive. (2002). *Privacy on and off the Internet: What consumers want.* (Report No. 15229). New York: Privacy & American Business.

Jöreskog, K. G., Sörbom, D., du Toit, S., & du Toit, M. (2001). *LISREL 8: New statistical features.* Lincolnwood, IL: Scientific Software International.

Jourard, S. M. (1971). *The transparent self*. New York: Litton Educational Publishing.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*(4), 1193-1294.

Kline, R. B. (1998). *Principles and practice of structural equation modeling.* New York: Guilford Press.

Lefcourt, H. M. (1991). Locus of control. In J. P. Robinson, P. R. Shaver, & L. S. Wrightsman (Eds.), *Measures of personality and social psychological attitudes* (pp. 413-500). San Diego, CA: Academic Press.

Lefcourt, H. M. (Ed.). (1981). *Research with the locus of control construct.* New York: Academic Press.

Levenson, H. (1981). Differentiating among internality, powerful others, and chance. In H. M. Lefcourt (Ed.), *Research with the locus of control construct: Vol. 1* (pp. 15-63). New York: Academic Press.

Louis Harris & Associates, (1999, October). *IBM multi-national consumer privacy survey.* Retrieved December 7, 2002 from http://www-1.ibm.com/services/files/privacy_survey_oct991.pdf

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods, 1*(2), 130-149.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-74.

Miller, A. R. (1971). *The assault on privacy: computers, data banks, and dossiers*. Ann Arbor, MI: University of Michigan Press.

Miller, L. C., & Read, S. J. (1987). Why am I telling you this? Self-disclosure in a goal-based model of personality. In V. J. Derlega, & J. H. Berg (Eds.), *Self-disclosure: theory, research, and therapy* (pp. 35-58). New York: Plenum Press.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 26*(4), 323-339.

Olmstead v. United States. (1928). 277 U.S. 438.

Petronio, S. S. (2002). *Boundaries of privacy: dialectics of disclosure*. Albany, NY: State University of New York Press.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2-17.

Post, R. C. (1989). The social foundations of privacy: Community and self in the common law tort. *California Law Review, 77*, 957-1010.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383-423.

Relyea, H. C. (2001). Legislating personal privacy protection: The federal response. *The Journal of Academic Librarianship, 27*(1), 36-51.

Rohrmann, B. (2002). *Risk attitude scales: Concepts and questionnaires.* Retrieved February 20, 2003, from http://www.psych.unimelb.edu.au/staff/br/rac-report.pdf

Rubin, P. H., & Lenard, T. M. (2002). *Privacy and the commercial use of personal information*. Norwell, MA: Kluwer Academic Publishers.

Rubin, R. R. (1994). Individualized Trust Scale. In R. R. Rubin, P. Palmgreen, & H. E. Sypher (Eds.), *Communication research measures: A sourcebook* (pp. 184-186). New York: Guilford Publications.

Schoeman, F. D. (1984). *Philosophical dimensions of privacy: An anthology*. New York: Cambridge University Press.

Schoeman, F. D. (1992). *Privacy and social freedom*. New York: Press Syndicate of the University of Cambridge.

Schumacker, R. E., & Lomax, R. G. (1996). *A beginner's guide to structural equation modeling.* Mahwah, NJ: Lawrence Erlbaum Associates.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18*, 21-32.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*, 1087-1156.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*, 1393-1462.

Spiekermann, S., Gorssklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *3rd ACM Conference on Electronic Commerce* (pp. 38-47). New York: ACM Press.

Spiekermann, S., Strobel, M., & Temme, D. (2005, February 23-25). *Drivers and impediments of consumer online information search: Self-controlled versus agent-assisted search.* Paper presented at Wirtschaftsinformatik 2005. Retrieved March 2, 2005, from http://www.wiwi.hu-berlin.de/~sspiek/WI05-Beitrag156.doc

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36-49.

Tardy, C. H. (1988). Self-disclosure: Objectives and methods of measurement. In C. H. Tardy (Ed.), *A Handbook for the study of human communication* (pp. 323-346). Norwood, NJ: Ablex Publishing Corp.

Warren, S. A., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*(1), 193-220.

Westin, A. F. (1981). *The dimensions of privacy*. New York: Garland Publishing.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Wheeless, L. R. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research, 4*(2), 143-157.

Wheeless, L. R., Erickson, K. V., & Behrens, J. S. (1986). Cultural differences in disclosiveness as a function of locus of control. *Communication Monographs, 53*(1), 36-46.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 338-346.

Wheeless, L. R., & Grotz, J. (1977). The measurement of trust and its relationship to self-disclosure. *Human Communication Research, 3*(3), 250-257.

Wilson, T. D. (2000). Human information behavior. *Informing Science, 3*(2), 49-56. Retrieved 11/2/2003 from http://inform.nu/Articles/Vol3/v3n2p49-56.pdf

Zeller, T., Jr. (2005, February 28). Breach points up flaws in privacy laws. *New York Times.* Retrieved February 28, 2005 from http://www.nytimes.com