Information Privacy: Measuring Individuals' Concerns About Organizational Practices[1]

By: H. Jeff Smith
Georgetown School of Business
Georgetown University
Old North Hall
Washington, D.C. 20057
U.S.A.
jsmith@guvax.georgetown.edu

Sandra J. Milberg
Georgetown School of Business
Georgetown University
Old North Hall
Washington, D.C. 20057
U.S.A.
milbergs@gunet.georgetown.edu

Sandra J. Burke
Georgetown School of Business
Georgetown University
Old North Hall
Washington, D.C. 20057
U.S.A.
burkes@gunet.georgetown.edu

Abstract

Information privacy has been called one of the most important ethical issues of the information age. Public opinion polls show rising levels of concern about privacy among Americans. Against this backdrop, research into issues associated with information privacy is increasing. Based on a number of preliminary studies, it has become apparent that organizational practices, individuals' perceptions of these practices, and societal responses are inextricably linked in many ways. Theories regarding these relationships are slowly emerging. Unfortunately, researchers attempting to examine such relationships through confirmatory empirical approaches may be impeded by the lack of validated instruments for measuring individuals' concerns about organizational information privacy practices.

To enable future studies in the information privacy research stream, we developed and validated an instrument that identifies and measures the primary dimensions of individuals' concerns about organizational information privacy practices. The development process included examinations of privacy literature; experience surveys and focus groups; and the use of expert judges. The result was a parsimonious 15-item instrument with four subscales tapping into dimensions of individuals' concerns about organizational information privacy practices. The instrument was rigorously tested and validated across several heterogenous populations, providing a high degree of confidence in the scales' validity, reliability, and generalizability.

Keywords: Privacy, LISREL, ethical issues, measures, reliability, validity

ISRL Categories: AI0401, AI0402, AI0403, AI0611, BD0104.01, BD0105

> It is inevitable that personal privacy will be one of the most significant pressure points...for most of the 1990s. Advancing technology, depersonalization of the workplace and other social environments, a growing population...all can be expected to create a greater personal need for a sense of space and dignity (Erwin Chemerinsky, as quoted in Smith, 1994).

[1] Allen Lee was the accepting senior for this paper.

Information privacy—"the ability of the individual to personally control information about one's self" (Stone, et al., 1983)—has been called one of the most important "ethical issues of the information age" (Mason, 1986; Smith, 1994). Public opinion polls show increasing levels of concern about privacy among Americans (Equifax, 1990; 1991; 1992; 1993; Katz and Tassone, 1990). For example, one survey indicates that 79 percent of Americans are concerned about threats to personal privacy, and 55 prcent feel that "protection of information about consumers will get worse by the year 2000" (Equifax, 1992). In addition, a number of corporations have faced legal problems and received negative media attention because of privacy issues (Cespedes and Smith, 1993; Culnan, 1993; Smith, 1994). In the United States, pressure for additional laws to guard against information privacy exposures is coming from both domestic and international quarters (Cespedes and Smith, 1993; Culnan, 1993). As organizations find their data management activities receiving more scrutiny from a privacy perspective, information systems managers should be aware of exposures and be accountable to their organizations (Straub and Collins, 1990).

Against this backdrop, research into issues associated with information privacy is increasing. Some privacy research dates back to the 1960s and 1970s (e.g., HEW, 1973; PPSC, 1977; Westin, 1967; Westin and Baker, 1972). Most of the scholarly work, however, has emerged during the 1980s and early 1990s. Consequently, it could be argued that the research stream is still in its infancy and that much work lies ahead as researchers examine the complex web of relationships in the information privacy domain. Based on a number of preliminary studies (Culnan, 1993; Milberg, et al., 1995; Smith, 1994; and Stone, et al., 1983), it has become apparent that organizational practices, individuals' perceptions of these practices, and societal responses are inextricably linked in many ways. Theories regarding these relationships are slowly emerging: for example, Stone and Stone (1990) developed a model for information flows and physical/social structures in work environments based on expectancy theory, Culnan (1993) tested an exploratory model that explains consumer attitudes toward some direct marketing practices, and Smith (1994) developed a model that explains corporate approaches to information privacy policymaking. Overall, however, the theoretical base is still quite fragmented, and few empirical tests of these relationships have been conducted.

Unfortunately, researchers attempting to examine such relationships through confirmatory empirical approaches may be impeded by the lack of validated instruments for measuring individuals' concerns about organizational information privacy practices. As in many other areas of information systems (IS) research (Jarvenpaa, et al., 1985; Straub, 1989), instrumentation issues have generally been ignored in the information privacy domain. This can lead to two potential problems over time: First, it will be difficult to assess the significance of *any particular study* because the "lack of validated measures in confirmatory research raises the specter that no single finding...can be trusted" (Straub, 1989, p. 148). Second, development of a *research stream* will become particularly problematic because it will be difficult to "compare and accumulate findings and thereby develop syntheses for what is known" (Churchill, 1979, p. 67). Thus, the frontiers of knowledge in privacy research can be extended by efforts to enhance the tools at researchers' disposal and to ensure that scientific rigor can be maintained in future studies.[2] Specifically, a rigorously validated instrument that measures individuals' concerns about organizational information privacy practices is needed because without such an instrument, researchers cannot credibly test explanatory theories regarding causal links between practices, individuals' perceptions, and societal responses. In addition, such an instrument will

[2] References to scientific rigor should not be interpreted as suggesting the superiority of confirmatory empirical research approaches over other approaches. The point being stressed is that *for researchers utilizing confirmatory empirical techniques*, the use of validated instruments is a critical factor. In addition, to the extent that the use of such instruments strengthens positivist research on a topic, this can also call for advances in interpretive research to be made on the same topic (Lee, 1991). See additional remarks in the "Discussion" section.

promote cooperative research efforts by "allowing other researchers in the stream to use this tested instrument across heterogenous settings and times" as well as by bringing "greater clarity to the formulation and interpretation of research questions" (Straub, 1989, p. 148).

To that end, this paper reports the results of a study that developed and validated a measurement instrument that can be used in future information privacy research. Table 1 shows the final product of our work: a 15-item instrument with four subscales (Collection, Errors, Unauthorized Secondary Use, and Improper Access; see definitions below) that measures individuals' concerns about organizational information privacy practices.

The following sections first consider the previous literature regarding individuals' concerns about organizational information privacy practices. They then detail the development and validation of the instrument and conclude with a discussion of implications for both researchers and managers.

Literature Review

A prerequisite step in the creation of a validated measurement instrument is a consideration of the dimensionality of the relevant construct (in this case, individuals' concerns about organizational information privacy practices). As one of several steps in this process, a thorough review of the existing literature was conducted[3] (Bearden, et al., 1993; Churchill, 1979).

It is common for information privacy to be approached as though it were a unidimensional construct. For example, while available opinion surveys (Equifax, 1990; 1991; 1992; 1993) report an increasing level of concern about information privacy, these surveys do not fully explore the nature (dimensionality) of those concerns.[4] Furthermore, while other studies have examined various dimensions underlying information privacy concerns, the specific dimensions differ from study to study,[5] and a common unifying framework relating these dimensions has not yet emerged. Thus, we attempted to ascertain the underlying dimensions—both central and tangential—that have been identified in either scholarly literature, in federal law, or in privacy advocates' writings.[6] Of course, this was a somewhat iterative process in that the understanding of the construct was refined in later steps (see "Methods" section below).

This exercise revealed several central dimensions of individuals' concerns about organizational information privacy practices: *collection* of personal information; *internal unauthorized secondary use* of personal information; *external unauthorized secondary use* of personal information; *errors* in personal information; and *improper access* to personal information. Two additional, tangential dimensions, which were mentioned with less frequency in the scholarly literature, were also noted: concerns regarding

[3] This section details the results of the literature review. In a later section ("Methods"), details of additional steps in this process are provided.

[4] For example, a commonly used public opinion survey question asks, "How concerned are you about threats to your personal privacy in America today?" (Equifax, 1990; 1991; 1992; 1993). While such a question provides valid data regarding levels of public concern, it provides no insight regarding the nature of the concerns.

[5] For example, Stone, et al. (1983) refer to collection, storage, usage, and release. Culnan (1993) utilized a 3x3 matrix, with acquire, use, and transfer along one axis and internal customer, external customer, and prospect along the other axis.

[6] An extensive literature review of information privacy research from prominent multidisciplinary publications and books provided an initial framework for the identification of the underlying dimensions of information privacy. To further our understanding of the dimensionality of information privacy concerns, a modified content analysis technique was used to identify concerns most often raised in privacy advocates' writings and in federal law. Following Kerlinger's (1986) outline, a "universe" consisting of approximately 960 articles in the publication *Privacy Journal* (a leading monthly publication for privacy advocates) from 1983-1990 was examined. A particular article was considered the unit of analysis. A beginning set of categories, inspired by the "Code of Fair Information Practices" as described in the U.S. Department of Health, Education, and Welfare study (1973) and the Privacy Protection Study Commission (PPSC, 1977), was used.

Table 1. Final Instrument

Here are some statements about *personal information*. From the standpoint of personal privacy, please indicate the extent to which you, *as an individual*, **agree** or **disagree** with each statement by circling the appropriate number.*

A. It usually bothers me when companies ask me for personal information.
B. All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.
C. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
D. Companies should devote more time and effort to preventing unauthorized access to personal information.
E. When companies ask me for personal information, I sometimes think twice before providing it.
F. Companies should take more steps to make sure that the personal information in their files is accurate.
G. When people give personal information to a company for some reason, the company should never use the information for any other reason.
H. Companies should have better procedures to correct errors in personal information.
I. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
J. It bothers me to give personal information to so many companies.
K. Companies should never sell the personal information in their computer databases to other companies.
L. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
M. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
N. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
O. I'm concerned that companies are collecting too much personal information about me.

Items A, E, J, and O comprise the "Collection" subscale; items B, F, H, and L comprise the "Errors" subscale; items C, G, K, and M comprise the "Unauthorized Secondary Use" subscale; and items D, I, and N comprise the "Improper Access" subscale. Subscale scores are calculated by averaging the responses to the items for each subscale; an overall score is then calculated by averaging the subscale scores.

* Each of the items is followed by a seven-point Likert scale anchored by "Strongly disagree" (1) and "Strongely agree" (7).

reduced judgment in decision making and *combining data from several sources*. Each is discussed briefly below (see synopsis in Table 2).

Collection

The Association for Computing Machinery (ACM), a major association of information processing professionals, has a phrase in its Code of Professional Conduct that dictates members shall "always consider the principle of the individual's privacy and seek . . . to minimize the data collected. . ." (ACM, 1980). This area of concern reflects the perception, "There's too much damn data collection going on in this society" (Miller, 1982). Individuals often perceive that great quantities of data regarding their personalities, background, and actions are being accumulated, and they often resent this. The growing collection of personal information has been a theme in privacy literature since the 1970s. Although Westin and Baker (1972) did not find that information collection had increased appreciably, they argued that it was an inevitable byproduct of the growing computer revolution and raised concerns in that regard. Shortly thereafter, two major reports from that era (HEW, 1973; PPSC, 1977) confirmed the trend and the concern; this position was echoed by Linowes (1989). Laudon (1986) also inferred a concern regarding excessive collection of data when he coined the moniker "dossier society" to describe our increasing reliance on personal data. In the behavioral literature, Stone, et al. (1983) utilized "information collection" as one component in their study; Stone and Stone (1990) also discuss a number of concerns associated with information collection.

Unauthorized secondary use (internal)

Sometimes information is collected from individuals for one purpose but is used for another, secondary purpose without authorization from the individuals. Even if contained *internally* within a single organization, unauthorized use of personal information will very often elicit a negative response. This concern was raised pointedly in the Code of Fair Information Practices, which was included in a seminal study sponsored by the U.S. Department of Health, Education, and Welfare (1973). Concerns about such secondary use were raised in several industry settings in a later study (PPSC, 1977) and echoed in Linowes (1989). Stone, et al. (1983) refers to this issue under the label of "information usage"; it is reiterated by Stone and Stone (1990) in a discussion of various information uses. Specific examples of such secondary, internal uses are also covered in the literature: for example, "sugging"—a practice in which data are collected ostensibly for research only to be used later for marketing purposes—falls into this area of concern (Cespedes and Smith, 1993). It is common for organizations to find new uses for data: for example, some banks' marketing groups have attempted to use income data collected on loan applications to sort customers into narrow categories for targeted sales offerings—a use of income data likely unanticipated by the customers at the time they filled in the loan application.

Unauthorized secondary use (external)

Some studies (for example, Tolchinsky, et al., 1981) have found that concerns about secondary use are exacerbated when personal information is disclosed to an external party (i.e., another organization). This issue was mentioned in studies conducted in the 1970s (HEW, 1973; PPSC, 1977; Westin and Baker, 1972), but it was not stressed in great depth at that time—perhaps because the technology of the day constrained such external exchanges of data. By the 1980s, though, the concern had become a major one. Linowes (1989) discusses several examples of unauthorized external use of information in various industries. Culnan (1993) examines attitudes toward external secondary uses in direct marketing applications. Stone, et al. (1983) consider the issue under the rubric of "information release," and Stone

Table 2. Dimensions

Dimension	Description of Concern	Major Literature References*
Collection	Concern that extensive amounts of personally identifiable data are being collected and stored in databases	HEW, 1973 Laudon, 1986 Linowes, 1989 Miller, 1982 PPSC, 1977 Stone, et al., 1983 Stone and Stone, 1990 Westin and Baker, 1972
Unauthorized Secondary Use (internal)	Concern that information is collected from individuals for one purpose but is used for another, secondary purpose (internally within a single organization) without authorization from the individuals	HEW, 1973 Linowes, 1989 PPSC, 1977 Stone, et al., 1983
Unauthorized Secondary Use (external)	Concern that information is collected for one purpose but is used for another, secondary purpose after disclosure to an external party (not the collecting organization)	Culnan, 1993 Linowes, 1989 Stone, et al., 1983 Tolchinsky, et al., 1981 Westin and Baker, 1972
Improper Access	Concern that data about individuals are readily available to people not properly authorized to view or work with this data	Date, 1986 Linowes, 1989 PPSC, 1977 (minor references)
Errors	Concern that protections against deliberate and accidental errors in personal data are inadequate	Date, 1986 HEW, 1973 Laudon, 1986 Miller, 1982 PPSC, 1977 (minor references) Westin and Baker, 1972
Reduced Judgment (tangential)**	Concern that automation of decision-making processes may be excessive and that mechanisms for decoupling from automated decision processes may be inadequate	Kling, 1978 Ladd, 1989 Laudon, 1986 Mowshowitz, 1976
Combining Data (tangential)***	Concern that personal data in disparate databases may be combined into larger databases, thus creating a "mosaic effect"	HEW, 1973 Laudon, 1986 PPSC, 1977

* Not an exhaustive list. Items in this column should be viewed as representative.

** While some authors have addressed Reduced Judgment in their scholarly writings, they have seldom identified it as a *privacy* concern, per se.

*** The Combining Data concern is almost always addressed in concert with either the Collection or the Unauthorized Secondary Use (External) concern.

and Stone (1990) discuss the "subsequent disclosures" of personal information.

The most commonly cited examples of this concern are the sale or rental of current or prospective customers' names, addresses, phone numbers, purchase histories, categorizations, etc., on mailing "lists," which are often transferred between the organizational entities as digital files. Trade publications in the direct marketing industry such as DM News ("DM" stands for "direct marketing") contain pages of advertisements for such lists (e.g., "individuals who responded to an advertisement for a weight-loss product").

Improper access

Who within an organization is allowed to access personal information in the files? This is a question not only of technological constraints (e.g., access control software) but also of organizational policy. It is often held that individuals should have a "need to know" before access to personal information is granted. However, the interpretation of which individuals have, and do not have, a "need to know" is often a cause of much controversy. PPSC (1977) and Linowes (1989) provide some attention to the topic—considering, for example, the inappropriate access to employees' healthcare records that are not controlled properly—and it is sometimes considered under the rubric of "security" in database literature (see, for example, Date, 1986). Of course, technological options now exist for controlling such access at file, record, or field level. But how those options are utilized and how policies associated with those uses are formed represent value-laden managerial judgments.

Errors

Many individuals believe that organizations are not taking enough steps to minimize problems from errors in personal data. Although some errors might be deliberate (e.g., a disgruntled employee maliciously falsifying data), most privacy-related concerns involve instead *accidental* errors in personal data. Early privacy studies detail some procedures for minimizing such errors (HEW, 1973; Westin and Baker, 1972; also see minor references in PPSC, 1977). Later works (Laudon, 1986; Linowes, 1989) document continuing problems in this domain.

Provisions for inspection and correction are often considered as antidotes for problems of erroneous data (HEW, 1973; PPSC, 1977; Smith, 1994). But many errors are stubborn ones, and they seem to snowball in spite of such provisions (Smith, 1994). In addition, a reluctance to delete old data—which can clearly become "erroneous" because of their static nature in a dynamic world—can exacerbate this problem (Miller, 1982). Also at issue are questions of responsibility in spotting errors: does a system rely on individuals to monitor their own files, or is there an overarching infrastructure in place (Bennett, 1992)? Although errors are sometimes assumed to be unavoidable problems in data handling, whether controls are or are not included in a system does represent a value choice on the part of the system's designers (Kling, 1978; Mowshowitz, 1976).

Reduced judgment

As organizations grow in size and in their data processing capabilities, they tend to rely more often on formulas and rules in their decision making (Cyert and March, 1963). Their use of automated decision-making processes may lead individuals to feel that they are being treated more as "a bunch of numbers" than as an individual. As systems are increasingly designed so that these decisions are automated, mechanisms for "decoupling" the decision making from the systems as appropriate—that is, reverting to human controls when the computer's limits as a decision maker are reached (Ladd, 1989)—should be included. When such mechanisms are not provided, concerns about this dimension of decision making increase (Kling, 1978; Ladd, 1989; Laudon, 1986; Mowshowitz, 1976). Some examples of this phenomenon border on the ridiculous:

American Express once issued a Gold Card to a man who had been dead 14 years, just because his widow filled in all the blanks on an application form. Much of the data would have appeared immediately suspicious to a human being (e.g., she entered all zeroes for his social security number and "God" as his employer), but the system apparently had been programmed to accept these entries, and the appropriate mechanisms for decoupling the decision making from the computerized information system had apparently not been included (Smith, 1994).

While advocates often couple "reduced judgment" with privacy in their arguments and writings, it should be noted that "reduced judgment" can easily be considered a tangential construct or even a separate construct of its own (under the rubric of "decision making"). Indeed, it has usually been referenced in scholarly work as a related concern rather than as a dimension of privacy, per se.

Combining data

Concerns are sometimes raised with respect to combined databases that pull personal data from numerous other sources, creating what has been termed a "mosaic effect." These combinations of data were mentioned in some of the 1970s privacy studies (HEW, 1973; PPSC, 1977) and in the 1980s (see especially Laudon, 1986). Even if data items in disparate databases are seen as innocuous by themselves, their combination into larger databases appears to some to be suggestive of a "Big Brother" environment. The Combining Data concern is usually encountered in the literature in parallel with Collection and/or Unauthorized Secondary Use (External) concerns and, in fact, may not be a separate dimension (see "Methods" below).

Methods

The ultimate objective of this research was the development and validation of an instrument to measure individuals' concerns about organizational information privacy practices. While it is expected that this instrument will be used primarily in positivist studies, the process of instrument development and validation used in this study included steps that addressed not only what Lee (1991) would call a researcher's positivist understanding (e.g., a theory taking the form of independent and dependent variables), but also the subjective understanding (i.e., what the research subjects themselves understand their situation to be) as well as a researcher's interpretive understanding (i.e., what the researcher observes and interprets to be the subjective understanding).[7]

As can be seen in Stage 1 of Figure 1,[8] an iterative process is used to (1) specify the domain and dimensionality of a construct, (2) generate a sample of items, and (3) assess content validity of these items (i.e., the extent to which scale items appear to be consistent with the theoretical domain/dimensionality of the construct (Churchill, 1979; Cronbach, 1971)).

Techniques[9] used to accomplish these tasks include literature reviews, experience surveys,[10] focus groups, expert judges, and pilot tests with relevant samples. During this stage, based on input from individuals, expert judges, and literature, scale items are trimmed and refined and dimensions may be added, deleted, or modified as understanding of the construct improves.

In Stage 2, the items and the conceptualization of the construct are subjected to "field

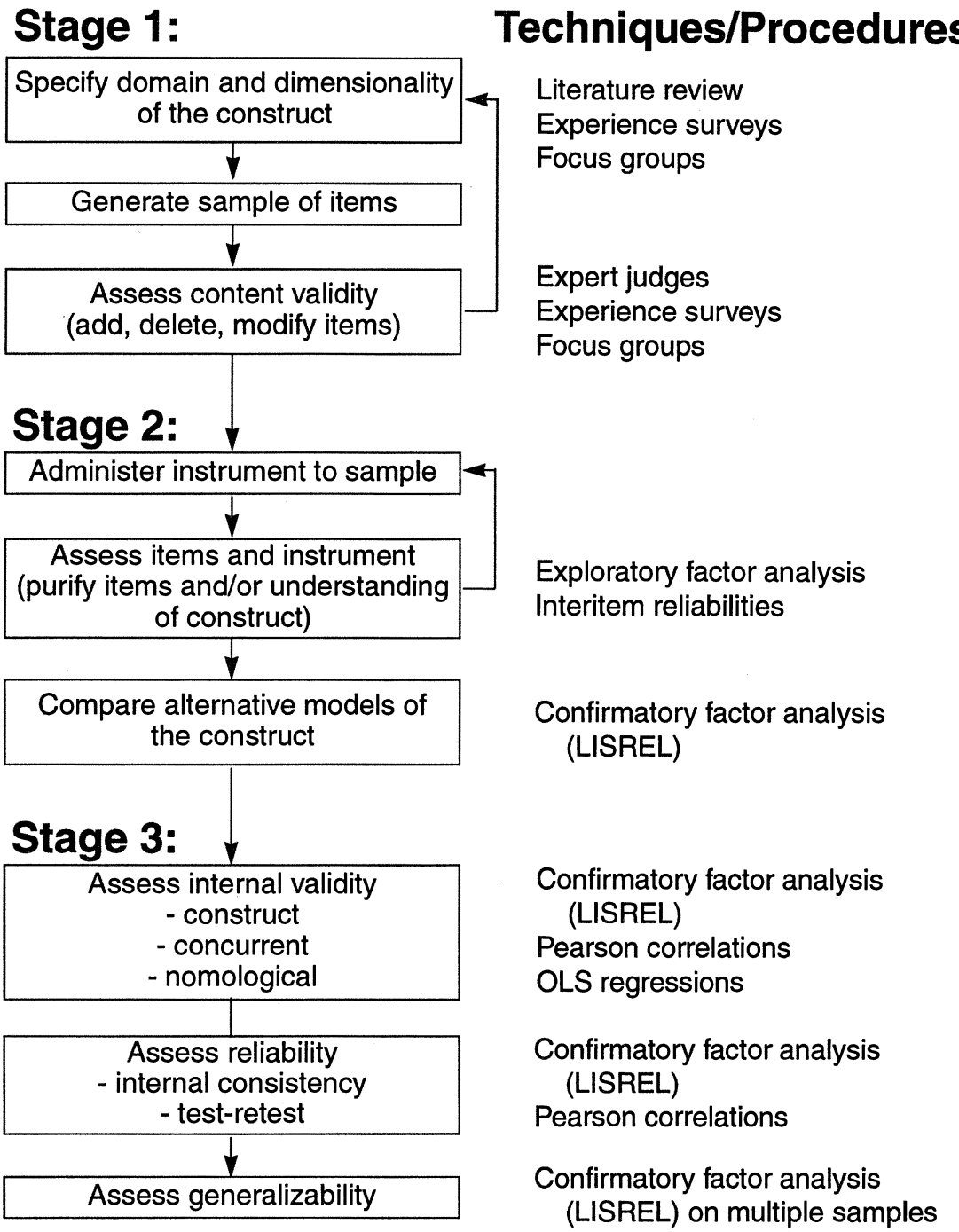
---

[7] See Lee (1991) for fuller explanations of these terms. Also, see remarks in our "Discussion" section.

[8] Figure 1 represents a synthesis and adaptation of several models of the development and validation process. It is not claimed to be a definitive model; however, it does include the steps that are widely accepted and have been used in past studies.

[9] For further discussion of these techniques, see Bearden, et al., 1993 and Churchill, 1979.

[10] An experience survey is "not a probability sample but a judgment sample of persons who can offer some ideas and insights into the phenomenon" (Churchill, 1979, p. 67).



Source: Adapted from Bagozzi (1980), Bearden, et al. (1993), Churchill (1979), and Straub (1989).

Figure 1. Instrument Development and Validation Process

tests." A preliminary version of the instrument is administered to various samples, and exploratory factor analysis is utilized to assess the items. The instrument is "purified" (Churchill, 1979) as researchers find that certain items should again be added, deleted, or modified. Indeed, the researchers may even find that they must modify their understanding of the construct's dimensionality. Stage 2 continues until the loading of the items in the exploratory factor analysis is consistent with the understanding of the construct's dimensions, *and* the inter-item reliabilities (Cronbach's alpha) are at satisfactory levels for all dimensions. In addition, Stage 2 includes a comparison of alternative models of the construct through confirmatory factor analysis (CFA). (See the Appendix for a discussion of the merits of CFA.)

In Stage 3, the internal validity of the instrument is assessed. This includes evaluations of the instrument's construct, concurrent, and nomological validity. Stage 3 also includes an assessment of the instrument's reliability, specifically *internal consistency* and *test-retest* reliability. Finally, Stage 3 includes an assessment of the instrument's generalizability (i.e., its usefulness for different populations). In all tests, the instrument must perform at statistically adequate levels. These levels have been documented, based on generally accepted criteria, by numerous writers (see Bagozzi and Yi, 1988; 1991; Bearden, et al., 1993; Bentler and Bonett, 1980; Fornell and Larcker, 1981) .

The following sections provide further detail regarding our instrument development process.

Instrument validation results—stage 1

To specify the domain/dimensionality of the "individuals' concerns about organizational information privacy practices" construct and to establish content validity of the generated scale items, the extensive literature review, detailed in a previous section, was used as a starting point in determining the central and tangential dimensions of the construct. Concomitant with this effort, semistructured interviews were conducted with 83 executives, managers, and employees of banks, insurance companies, and a credit card issuer.[11] Further, 18 consumers were interviewed either individually or in focus groups. (See Table 3a for a description of the samples; see Table 3b for a summary of the procedures and results in this study.)

By discussing the construct both with people who were employed in organizations handling much personal data and with people who were not in any way associated with such organizations, we were better able to interpret the subjective understanding (i.e., what the individuals themselves understood "concerns about information privacy" to mean). To achieve our own interpretive understanding, rather than rely exclusively on how other researchers and some advocates have already interpreted what individuals themselves understand information privacy to mean (see previous discussion under "Literature Review"), we interviewed 12 consumer/privacy advocates either in person or over the phone.

Commonly cited themes regarding information privacy concerns from the research articles, from privacy advocates' writings and U. S. laws, and from the interviews/focus groups were sorted in an iterative and interpretive process by the researchers, and the categories were combined and modified in an intuitive manner to suggest underlying dimensions. Based on the dimensions identified, we generated a preliminary set of 72 survey items for measuring individuals' concerns about organizational information privacy practices.

To establish *content validity* of the scale items (i.e., whether the items truly sampled the universe of situations we were attempting to mea-

[11] In all interviews, organizations' employees were asked for their opinions both as employees *and* as individuals. While better informed about organizational practices than average consumers, employees were usually able to distinguish between their organizational perspectives and their personal opinions.

Table 3a. Samples

Sample #	n of sample*	Composition of Sample	Date Collected
1	83	Executives, managers, employees—banks, insurance organizations, credit card issuer	Fall 1989/Spring 1990
2	18	Consumers (individual and focus group)	Spring 1990
3	12	Consumer/privacy advocates	Spring 1990
4	3	Judges (familiar with privacy area)	Spring 1990
5	15	Doctoral students and faculty members (large Eastern university)	Spring 1990
6	15	Organizational employees (follow-up interviews)	Spring 1990
7	25	Employees—bank, insurance organizations (focus groups)	Spring 1990
8	704	Employees—bank, insurance organizations, credit card issuer	Spring /Summer 1990
9	239	Information systems managers; graduate business students (two Eastern universities)	Summer/Fall 1991
10	270	Graduate business students (four geographically dispersed U.S. universities)	Spring 1992
11	147	Graduate business students (Eastern university)	Fall 1992
12	354	U.S.-based ISACA members	Spring 1993
13	186**	Undergraduate business students (Eastern university)	Spring 1993
14	170***	Undergraduate business students (Eastern university)	Fall 1993
15	77	Graduate business students (two geographically dispersed U.S. universities)	Fall 1993

* n's reported in this table are for the *total* samples. These n's may differ slightly from those in subsequent tables, which report *effective* sample sizes (in which responses with some missing data have been removed).

** All 186 of these students completed a "test" of the instrument, and these 186 responses were used for the "generalizability" exercise. One hundred twenty-three of the 186 also completed the retest" of the instrument eight weeks later) and were used in the "test-retest" exercise. Half of the retest" group was randomly selected to complete a "cynical distrust" scale; 59 of these, who had also completed the "test," were correlated with the "cynical distrust" scale.

*** These 170 students were randomly assigned to complete, in addition to the information privacy instrument, either a "paranoia" or a "social criticism" scale.

Table 3b. Procedures and Results

Stage*	Task	Technique/ Procedure	Samples (See Table 3a)	Results
1	Interpret organizational participants' understanding of matters pertaining to construct domain and dimensionality	Semistructured interviews	1, 2	Preliminary research understanding of construct domain and dimensionality.
1	Improve interpretation of the organizational participants' understanding of matters pertaining to construct domain and dimensionality	Semistructured interviews	3	Refined research understanding of construct domain and dimensionality; used in generating set of 72 survey items.
1	Assess content validity of initial item set	Judging exercise	4	33 items discarded, resulting in a 39-item set.
1	Test content validity of reduced item set	Judging exercise	5	Items deleted and reworded, resulting in a new 32-item set.
1	Test refinement of construct domain and dimensionality	Follow-up interviews	6	Confidence in refined understanding of construct domain and dimensionality.
1	Pilot test preliminary survey	Focus group: fill in survey and discuss	7	Items deleted and reworded, resulting in a new 20-item set.
2	Assess items and instrument	Exploratory factor analysis and interitem reliabilities	8	20 items included on instrument. Deleted 3, added 2, and modified 8 for clarity, resulting in a 19-item instrument.
			9	19 items included on instrument. Deleted 2, added 8, and modified 6 for clarity, resulting in a 25-item instrument.
			10	Secondary internal and external use converged into a single dimension. Also deleted items that did not clearly load onto single factors and items that were redundant, resulting in a 15-item instrument (see Table 1). Of these 15

Table 3b. continued

				items, all loaded unambiguously onto four factors; Cronbach's alphas at adequate levels.
2	Compare alternative models of the construct	Confirmatory factor analysis (LISREL)	10	Hypothesized 4-factor model provided best fit to data compared to alternative models (see Table 4)
3	Assess construct validity — overall model fit	Confirmatory factor analysis (LISREL)	11	Non-centralized normed fit index adequate
3	Assess construct validity — convergent/ discriminant	Confirmatory factor analysis (LISREL)	11	Standardized factor loadings, average variance extracted, and factor inter-correlations adequate (see Tables 6 and 7)
3	Assess concurrent validity	Pearson correlations	12	Significant correlations with public opinion questions
3	Assess nomological validity	OLS regressions	15	Expected relation-ships with past experiences and prior knowledge supported
		Pearson correlations	13, 14	Expected relation-ships with personality factors supported
		Pearson correlations	15	Expected relation-ships with future behavioral intentions supported
3	Assess reliability — internal consistency	Confirmatory factor analysis (LISREL)	11	Composite reliability, average variance extracted adequate (see Table 6)
3	Assess reliability — test-retest	Pearson correlations	13	Significant correlations over an 8-week period
3	Generalizability	Confirmatory factor analysis (LISREL)	12, 13	Validity and reliability shown for disparate populations (see Table 8)

* As shown in Figure 1.

sure (Cronbach, 1971; Straub, 1989)), we asked three judges, familiar with the privacy area, to screen the 72 items for those that did not appear consistent with the construct and the identified dimensions (i.e., did not appear to actually measure individuals' concerns about organizational information privacy practices).[12] This resulted in a reduced set of 39 items. Then, 15 doctoral students and faculty members at a large Eastern university judged this reduced set of items. Specifically, the dimensions were explained to eight of the doctoral students/faculty members, who were asked to evaluate the items for their applicability to the respective dimensions. The other seven doctoral students/faculty members were presented with the items but were not given an explanation of the dimensions. They indicated, for each item, what they perceived that item would measure. Items that were either inconsistently classified or were misclassified were eliminated or reworded. After this analysis, 32 items remained.

Following this step, follow-up interviews were conducted with 15 corporate employees. In addition, at this point, the items were presented to 25 people employed by banks and insurance organizations. Using a focus group format, participants filled in the survey and then discussed their reaction to, and thoughts about, each item. Based on this test, further modifications and reductions resulted in a 20-item scale.

During this iterative process, as defined in Stage 1, the domain and the dimensionality of the "individuals' concerns about organizational information privacy practices" construct were repetitively assessed and modified. It became apparent that the Combining Data dimension was actually subsumed by two other dimensions: Collection and Unauthorized Secondary Use (External). Further probing with both advocates and consumers revealed that Combining Data concerns are actually viewed as an *outcome* of Collection and Unauthorized Secondary Use (External). When we tested some items that purported to measure concerns about Combining Data, our judges consistently held that it was almost impossible to separate the items' content from the Collection and Unauthorized Secondary Use (External) dimensions. Also during this process, Reduced Judgment was found by our judges and by some consumers to be tangential to the major construct of concern about information privacy and was dropped from further consideration. Few scholarly works hold Reduced Judgment to be a dimension of privacy. Furthermore, privacy advocates, when pressed, were inclined to concede that Reduced Judgment was actually outside the sphere of *privacy* concerns, per se.

Instrument validation results—stage 2

Stage 2 includes a preliminary assessment and refinement of the instrument through exploratory methods. In particular, in our study, the 20-item scale was administered to a sample of 704 bank, insurance organization, and credit card issuer employees.[13] Exploratory factor analysis and interitem reliability (Cronbach's alphas) provided tentative support for the various dimensions. Unfortunately, however, several items did not load as expected. An additional iterative process was initiated in which three versions of revised instruments were administered to varied populations, such as information systems managers and graduate business students.

Based on additional exploratory factor analysis, items were deleted, added, or revised. This process eventually resulted in a 15-item instrument. Four factors emerged representing

[12] For example, when presented with some preliminary items that were attempting to measure concerns about Reduced Judgment, the judges responded that they had difficulty in understanding why it was a privacy concern, per se.

[13] The survey was distributed to the employees, who were randomly chosen from the organizations' personnel rosters, under a cover letter from a senior executive. The completed, anonymous surveys were mailed directly to the researcher. A total of 1,103 surveys were distributed, and 704 were returned, for a response rate of 63.8 percent. The survey instructions said "We are interested in your own, *personal* opinions about the issue of privacy. Your responses will be held in complete anonymity."

the subscales: Collection (4 items), Errors (4 items), Unauthorized Secondary Use (4 items), and Improper Access (3 items). Examination of the exploratory factor analysis revealed that the unauthorized **internal** secondary use and the **external** secondary use dimensions had converged onto a single factor, the salient feature being that the secondary use of the information had not been authorized by the individuals involved. Chosen items all had factor loadings greater than .60 on the same factor in all factor analyses performed. (The final instrument is shown in Table 1.)

Stage 2 included one final step: to determine whether the hypothesized model of a four-dimension construct provided the best fit to the data as compared to alternative plausible models. To accomplish this, the overall fits of four theoretically plausible alternative models (a unidimensional model, a three-dimensional model, a model with two main factors and three sub-factors, and the hypothesized four-factor model) were compared using the CFA program LISREL (Joreskog and Sorbom, 1984). Four statistics provided in the LISREL program that are commonly used to compare model fits are the non-adjusted and adjusted goodness-of-fit indices (GFI and AGFI, respectively), root mean square residuals (RMR), and chi-square statistics (Bagozzi and Yi, 1988).

Comparison of these statistics (see Table 4) suggests that the hypothesized four-factor model performs better on the overall model fit measures than competing models. The chi-square statistics for all models estimated were significant, but—given the large samples used in the study—the significant chi-squares were likely artifacts of sample size (Bentler and Bonett, 1980) . Thus, a comparison of the GFI, AGFI and RMR measures—which are independent of sample size (Bagozzi and Yi, 1988)—was performed to assess the model's fit. As shown in Table 4, both the GFI and the AGFI of the four-factor model are higher than those for the three competing models. Further, RMRs are also considerably higher in the competing models (more residual variance remains) than in the hypothesized model. Finally, the coefficient of determination, a criterion for evaluating the global fit of a model by assessing explained variance (i.e., how well the items serve as joint measures of the latent variable), was examined. As shown in Table 4, the coefficient of determination is as high or higher in the four-factor model as in the other three models. Thus, of the four models compared, the hypothesized four-factor model provided the best fit to the data and was ultimately accepted.

Instrument validation results—stage 3

Stage 3 included assessments of the instrument's internal validity, its reliability, and its generalizability.

Table 4. Comparison of Four Models

	One-Factor Model	Three-Factor Model	Second-Order Model	Four-Factor (Hypothesized) Model
Chi-square (d.f.)*	792 (90)	371 (101)	371 (101)	240 (84)
GFI	.66	.75	.85	.90
AGFI	-.36	.42	.42	.67
RMR	.10	.07	.066	.047
Coeff. of Determination	.812	.991	.970	.996

* p<.001 for all models tested.

Internal Validity

Construct Validity

Construct validity is defined as the extent to which the operationalization of a construct measures what it is supposed to measure (Cook and Campbell, 1979). To establish construct validity, we considered (1) the adequacy of the model's fit and (2) convergent and discriminant validity for the model. To this end, the instrument was administered to a new sample of graduate business students (n=147).[14]

Adequacy of Model's Fit: In Stage 2, it was shown that the four-factor model provided the best fit to the data, suggesting its superiority over the other models in defining the "individuals' concerns about organizational information privacy practices" construct. However, the accepted model will achieve an adequate or satisfactory fit to the data only when a significant degree of correspondence exists between concepts and their respective measures and when measurement error is random (Bagozzi and Phillips, 1982). If significant measurement or method errors (or other external confounding factors) are present, overall model fit will be poor, suggesting model misspecification. In other words, subject responses must fit a fairly well-defined pattern for the hypothesized model to be sustained and construct validity supported.

On that basis, the first step in assessing construct validity using the CFA technique is to assess overall model fit. While the chi-square statistic provided in LISREL is often used to assess the adequacy of the model's fit, it may be a misleading artifact of sample size (Bentler and Bonett, 1980). Given the large sample size in this study, the overall fit of the model was examined using the non-centralized normed fit index (NCNFI). The NCNFI, which is independent of sample size (Bentler, 1990; McDonald and Marsh, 1990), assesses the proportion of additional variance explained in the hypothesized model as compared to a null model that hypothesizes that all variables are mutually independent.[15] This analysis is commonly performed to assess model fit when the CFA does not fulfill the acceptance criterion of a non-significant chi-square statistic, even though other measures of model fit fall within acceptable ranges (Bagozzi, 1993; Bentler, 1990; McDonald and Marsh, 1990), as was found in this case.

The NCNFI for this model is .91, which is greater than the .90 rule of thumb recommended as a minimum satisfactory level (Bentler and Bonett, 1980), suggesting adequate model fit from a practical standpoint. In other words, the remaining incremental fit that could be achieved by additional model modifications is small. Further, the coefficient of determination (which shows how well the hypothesized relations account for the factors) is very high at .996. Finally, the RMR is also very low, at .065 (Bagozzi and Yi, 1988). These findings support the overall adequacy of the model fit and provide support for the theoretical structure of the construct (Bagozzi and Yi, 1988).

Convergent and Discriminant Validity: Convergent validity refers to the extent to which multiple measures of a construct agree with one another (Campbell and Fiske, 1959). Discriminant validity refers to the extent to which measures of different constructs are distinct (Campbell and Fiske, 1959). A traditional method for assessing construct validity has been the multitrait-multimethod (MTMM) matrix. However, CFA affords certain advantages in validity assessment over MTMM matrix analysis (Bagozzi and Phillips, 1982). CFA explicitly represents random measurement error and allows for estimation of method variation. In addition, it provides explicit tests of the entire model, estimates of parameters, and a variety of fit measures, not available with the MTMM procedure (Bagozzi, 1993).

There are several approaches to assessment of convergent validity through CFA. First, con-

[14] Loadings from an exploratory factor analysis and the interitem reliabilities for this sample are shown in Table 5.

[15] The method for calculating the NCNFI is specified in Bentler (1990, pp. 239-241). The chi-square for the null model was 1094 (d.f. = 105).

Table 5. Final Instrument—Factor Analysis

Item #	COLLECTION Factor Loading	ERRORS Factor Loading	UNAUTHORIZED SECONDARY USE Factor Loading	IMPROPER ACCESS Factor Loading
J	.861			
E	.856			
A	.855			
O	.762			
F		.864		
H		.816		
L		.811		
B		.679		
K			.778	
M			.768	
G			.719	
C			.717	
N				.773
D				.771
I				.719

These results are from a sample of 147 business graduate students from Fall 1992. All loadings above .40 are listed above.
Interitem reliabilities (Cronbach's alpha): Collection, .88; Errors, .84; Secondary Use, .80; Improper Access, .75.

vergence implies that all within-construct correlations are both high and of approximately the same magnitude (Fornell and Larcker, 1981). To assess this aspect of convergent validity, the fit of the internal structure of the model (as discussed above), factor loading size, and significance were assessed. Bagozzi and Yi (1991) suggest weak evidence of convergent validity results when the factor loading on an item of interest is significant. Strong evidence is achieved when the squared factor loading is greater than .5 (more than half of the total variation in the measures is due to the trait). As shown in Table 6, standardized factor loadings (SFL) for all measures are greater than .6; all are statistically significant at $p<.05$. In addition, 12 of the 15 items have squared factor loadings greater than .5.

Second, convergent validity can be assessed in terms of the degree to which the four subscales (which might be considered four different measures of concern) are correlated (Bagozzi, 1980; Barki and Hartwick, 1994). Thus, to further assess convergent validity, the correlations between the subscales were examined. As shown in Table 7, the correlations between the dimensions are all significantly different from zero ($p<.05$). This suggests that the four dimensions are all measuring some aspect of the same construct (are not orthogonal).

To assess discriminant validity, subscales must be examined to insure they are not perfectly correlated (correlations equal to 1). As shown in Table 7, all subscale correlations are significantly different from one ($p<.05$). This suggests that while the subscales are measuring aspects of the same construct, they are measuring unique dimensions of that construct. Further, more rigorous evidence of discriminant validity is also observed by looking at the average variance extracted (AVE) by each factor relative to that factor's shared variance with other factors in the model (see Fornell and Larcker, 1981). (AVE measures the amount of variance that is captured by the construct in relation to the

amount of variance due to measurement error.) In every case, the AVE associated with a factor (see Table 6) is greater than the shared variance (squared correlation) between that and every other factor (see Table 7).

Concurrent Validity

Concurrent validity is considered when one test is proposed as a substitute for another or if the test is shown to correlate with some useful criterion (e.g., another test) administered at the same time (Cronbach and Meehl, 1955; Bagozzi, 1981). To assess concurrent validity of this instrument, the correlation between responses to the current instrument and responses to previously utilized public opinion survey questions was assessed. These public opinion surveys (see Cambridge Reports, 1989; Equifax, 1990; 1991; 1992; 1993; Katz and Tassone, 1990) typically used questions

Table 6. Summary of Parameter Estimates of Four-Factor Model

Factor	Item	Graduate Business Students (n= 147)		
		SFL	CR	AVE
Collection	A	.816		
	E	.743		
	J	.870		
	O	.765		
			.88	.69
Errors	B	.700		
	F	.709		
	H	.720		
	L	.900		
			.85	.58
Secondary Use	C	.726		
	G	.669		
	K	.646		
	M	.781		
			.80	.50
Improper Access	D	.652		
	I	.733		
	N	.721		
			.75	.50
Chi-Square		174 (84)		
NCNFI		.91		
RMR's		.065		
Coeff. Determ.		.996		

Legend: SFL = Standardized Factor Loading
CR = Composite Reliability
AVE = Average Variance Extracted
NCNFI = Non-centralized Normed Fit Index
RMR = Root Mean-squared Residual

Table 7. Factor Intercorrelations of Four-Factor Model

FACTORS	Collection	Errors	Unauthorized Secondary Use	Improper Access
Collection	1.00			
Errors [Squared Correlation] (Std. Dev. of Correlation)	.216 [.047] (.09)	1.00		
Unauthorized Secondary Use [Squared Correlation] (Std. Dev. of Correlation)	.425 [.181] (.08)	.448 [.201] (.08)	1.00	
Improper Access [Squared Correlation] (Std. Dev. of Correlation)	.264 [.070] (.10)	.611 [.373] (.07)	.641 [.411] (.08)	1.00

All factor intercorrelations are significantly different from zero ($p<.05$) and one ($p<.05$).
These results are from a sample of 147 business graduate students from Fall 1992.

that have been subjected to limited validation procedures, and the questions address general, unidimensional privacy concerns. Nevertheless, it is expected that a strong relationship should exist between a subject's responses to those questions and the scale developed in this research. To check this, three questions that had been used on previous public opinion surveys were included with our instrument, and this combined survey was administered to a sample of 354 U.S.-based members of the Information Systems Audit and Control Association (ISACA).[16] The three questions were:

1. "Compared with other subjects on your mind, how important is personal privacy?" (Cambridge Reports, 1989).

2. "How concerned are you about threats to your personal privacy today?" (Equifax, 1990; 1991; 1992; 1993).

3. "As computer usage increases in business and the general society, more and more information on individual consumers is being acquired and stored in various computers. How serious a threat to personal privacy is this development?" (Cambridge Reports, 1989).

Correlations between each subject's response to these questions and their overall score on our instrument were .35, .36, and .46 for items (1), (2), and (3), respectively ($p < .001$ for all three). The expected relationship between public opinion survey questions and the current instrument was observed.

Nomological Validity

Nomological validity refers to the extent to which predictions based on the construct being measured are confirmed within a wider theoretical context or network of constructs (Bagozzi, 1981; Cronbach, 1971; Cronbach and Meehl, 1955). Not often tested in IS research (see, however, Straub, et al., 1995), nomological validity examines the robustness of the constructs as they interrelate with one another. To assess nomological validity, we considered (1) some possible antecedents that might affect levels of information privacy concern, (2) individual factors that might have

[16] ISACA members were asked to respond "as an individual" and to give their "personal opinions." In a later section ("Generalizability"), results of a CFA assessment of the ISACA members' responses to our instrument are described.

theoretical relationships to levels of concern, and (3) some future behavioral intentions that should be associated with levels of concern.

Antecedents: Two theoretically plausible "causal" variables were assessed. It has been suggested that (a) previous personal experiences may impact one's concerns about information privacy (Culnan, 1993; Stone and Stone, 1990), and (b) media coverage may increase the level of concern about information privacy (Westin, 1990). These assertions lead to a reasonable set of propositions. It was proposed that individuals who had been exposed to, or been the victim of, personal information misuses should have stronger concerns regarding information privacy. To that end, 77 business graduate students from two geographically dispersed U.S. universities were asked to complete our instrument and were also asked to answer the following questions (on seven-point Likert scales) (1) "How often have you personally been the victim of what you felt was an improper invasion of privacy?" and (2) "How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers?"[17] The first question examines, to some degree, the respondent's perception of his or her own experiences with respect to information handling. The latter question examines the respondent's level of knowledge regarding collection and use of personal information. Results of regression analyses, with overall concern as the dependent variable and experience and knowledge as independent variables, strongly support these research propositions, with beta coefficients of .16 and .22, respectively ($p < .01$ for both).

Individual Personality Factors: Prior research has suggested that information privacy concerns may also be associated with various personality factors (e.g., Berscheid, 1977; Cozby, 1973; Kelvin, 1973; Laufer and Wolfe, 1977; Levin and Askin, 1977; Stone, 1986; Warren and Laslett, 1977). Some factors that one might expect to be correlated with information privacy concerns include: (1) trust/distrust, (2) paranoia, and (3) social criticism. Therefore, the instrument was administered in conjunction with scales measuring the suggested related personality factors to separate samples of undergraduate business students as follows:

It is argued that cynical distrust may be positively correlated with concern for information privacy in that individuals with high levels of distrust may also be more concerned about the use and dissemination of their personal information. Examination of the responses to the "cynical distrust" and the "overall level of concern" scales supports this contention (n = 59,[18] correlation = .30,[19] $p < .05$).

Paranoia is a second personality trait argued to be positively correlated with concern for information privacy. It is plausible that individuals who are paranoid are also likely to be more concerned about the privacy of their personal information. When both the paranoia scale (Fenigstein and Vanable, 1992) and the information privacy concern scale were administered to undergraduates, a significant correlation was observed (n = 87, correlation = .37, $p < .001$).

The social criticism scale measures "the degree of acceptance or rejection of the values, norms, and practices of...society" (Jessor and Jessor, 1977). It is proposed that consumers who reject society's values, norms, and practices would also be highly concerned about information privacy. Correlational analysis of responses to the information privacy concern instrument and the social criticism scale showed support for this proposition (n = 83, correlation = .37,[20] $p < .001$).

[17] Both of these questions were patterned after those in Equifax (1990).

[18] Students in this sample were also used in the test-retest reliability exercise (see section below). They responded to the "cynical distrust" scale following the "retest" of the privacy concern instrument. The reported correlation utilizes the "test" score for the privacy concern instrument (completed eight weeks earlier).

[19] The correlations in this section refer to our OVERALL scale.

[20] This correlation is reported as an absolute value; its direction is consistent with the proposition.

Future Behavioral Intentions: Previous research (e.g., Stone, et al., 1983) suggests that individuals with higher levels of concern about information privacy practices may be more likely in the future to refuse to participate in activities that require the provision of personal information. They may also be more likely to contact official agencies or companies regarding information practices. To provide a preliminary test of such assertions, the 77 business graduate students from two geographically dispersed U.S. universities (see "Antecedents" section above) were given, in addition to the information privacy instrument, a set of six items that investigated such future behavioral intentions with respect to information privacy.[21] The six items exhibited a high level of interitem reliability (Cronbach's alpha = .87). A mean score for the six items was correlated with the overall scale score for our instrument. The research proposition suggesting that higher levels of information privacy concern will be associated with stronger intentions to take privacy-related actions was strongly supported (correlation = .33, $p<.01$).

Reliability

The reliability of the instrument was assessed by evaluating (1) internal consistency and (2) test-retest reliability.

[21] Respondents were asked how likely they were, within the next three years, to: (1) "decide not to apply for something, like a job, credit, or insurance, because you do not want to provide certain kinds of information about yourself," (2) "refuse to give information to a business or company because you think it is too personal," (3) "take action to have your name removed from direct mail lists for catalogs, products, or services," (4) "write or call a company to complain about the way it uses personal information," (5) "write or call an elected official or consumer organization to complain about the way companies use personal information," and (6) "refuse to purchase a product because you disagree with the way a company uses personal information." Each was followed by a seven-point Likert scale anchored by "very likely" and "very unlikely." Some of these questions were patterned after those in Equifax (1990).

Internal Consistency

Internal consistency examines the degree to which the "items used to assess a construct reflect a true, common score for the construct" (Bagozzi, 1980; Barki and Hartwick, 1994). To assess internal consistency in this research, two measures were calculated in addition to factor loadings: (1) composite reliability (CR) of the dimension measures and (2) AVE from the dimension measures. CR considers the ratio of non-random variation associated with all measures of a subscale to total variation in all these measures. As shown in Table 6, CRs for the dimension measures are all quite high and well above a .6 rule of thumb of acceptability (Bagozzi and Yi, 1988).

AVE, as described earlier, measures the amount of variance captured by the construct in relation to the amount of variance attribued to measurement error. If AVE is less than .5, the variance associated with measurement error is larger than the variance captured by the construct, and the construct reliability is questionable. As shown in Table 6, AVEs are all at or above .5, which is a rule of thumb for adequacy of this measure (Bagozzi and Yi, 1988). Thus, the measures of internal reliability and structure fit all surpass the minimum standards of adequacy.

Test-Retest Reliability

Test-retest reliability examines an instrument's ability to achieve stable responses from a single sample over time (Churchill, 1979). To assess the test-retest reliability of our instrument, it was administered on two separate occasions to a single sample of undergraduate business students. Specifically, 123 students (of 186 total) responded to both the "test" and "retest" of the instrument, which were separated by a period of eight weeks. Correlations for these repetitions for the four subscales ranged from .63 to .74, and the correlation for the overall scale was .78 ($p<.001$ for all), which is in line with acceptable levels reported in prior, similar scale development research (Bearden, et al., 1993). Test-retest

correlations for individual *items* ranged from .39 to .66 ($p < .001$ for all).

Generalizability

To achieve its full usefulness, an instrument should be applicable to "other subjects, other groups, and other conditions" (Kerlinger, 1986, p. 299). Such a concern is included under the rubric of "external validity," which is defined as "persons, settings, and times to which findings can be generalized" (Straub 1989). While our instrument was initially based upon input from numerous sources (as described in Stage 1), it must also be validated with different populations. To achieve generalizability of the instrument, it was administered to, and validated with, two diverse sample populations in addition to the sample of graduate business students: undergraduate business students (n= 186) and U.S.-based members of the ISACA (n= 354).[22] As can be seen in Table 8, the results of CFA analyses on data from these samples supports the validity and reliability of the instrument across these populations as well. Specifically, the validation of the instrument across two groups as dissimilar as undergraduate students (who have, arguably, a low level of understanding regarding actual industry practices) and IS auditors (who, arguably, should represent a population with high on-the-job knowledge) stands as strong evidence of the instrument's generalizability (Gordon, et al., 1986).

Additional Findings

The relationships between the subscales and individuals' response patterns seem to provide additional insights into the underlying nature of the information privacy concern construct. As can be seen in Table 9, there may be a hierarchy of concern regarding the various dimensions. It was observed that the highest levels of concern were associated with Improper Access and Unauthorized Secondary Use. Lower levels of concern were associated with Collection and Errors. Within these categories, however, there seem to be some distinctions between samples (see Table 9). For example, ISACA members ranked Unauthorized Secondary Use as their top concern, while the other respondents indicated more concern about Improper Access.

[22] The ISACA sample was also utilized for some tests of nomological validity; this student sample was also utilized for the "test-retest" evaluation and for one test of nomological validity (correlation with "cynical distrust") (see Tables 3a and 3b).

Discussion

This study provides two major contributions to the privacy literature: (1) a framework describing the primary dimensions of individuals' concerns about organizational information privacy practices and (2) a validated instrument for measuring those concerns. The development process included examinations of privacy literature and U.S. laws; experience surveys and focus groups; and the use of expert judges. The result was a parsimonious 15-item instrument with four subscales tapping into dimensions of individuals' concerns about organizational information privacy practices. The instrument was rigorously tested and validated across several heterogenous populations, providing a high degree of confidence in the scales' validity, reliability, and generalizability.

Before considering implications for researchers and managers, two limitations of this study should be noted. First, all scale development processes require a number of "judgment calls" by researchers based on their analysis of the literature; on input from experience surveys, focus groups, and expert judges; and on levels of acceptability for various statistical measures. In particular, based on input from various sources, we concluded that one of the dimensions, Combining Data, was actually represented by two of the other dimensions, Unauthorized Secondary Use (External) and Collection. We also concluded that Reduced Judgment was not a part of the major "individuals' concerns about organiza-

Table 8. LISREL Results for Generalizability

Factor	Item	Undergraduate Business Students (n=186)			IS Auditors (n=354)		
		SFL	CR	AVE	SFL	CR	AVE
Collection	A	.675			.759		
	E	.559			.772		
	J	.941			.878		
	O	.689			.667		
			.81	.53		.86	.60
Errors	B	.647			.637		
	F	.841			.864		
	H	.698			.775		
	L	.857			.890		
			.85	.59		.87	.64
Unauthorized Secondary Use	C	.691			.733		
	G	.636			.726		
	K	.671			.693		
	M	.898			.838		
			.82	.54		.84	.56
Improper Access	D	.691			.785		
	I	.754			.598		
	N	.877			.880		
			.82	.65		.80	.58
Chi-Square		139 (84)			330 (84)		
NCNFI		.96			.91		
RMR's		.063			.074		
Coeff. Determ.		.998			.998		

Legend: SFL = Standardized Factor Loading
CR = Composite Reliability
AVE = Average Variance Extracted
NCNFI = Non-centralized Normed Fit Index
RMR = Root Mean-squared Residual

Table 9. Subscales

Subscale	Mean (S.D.) for MBAs (n = 146)	Mean (S.D.) for Undergraduates (n = 183)	Mean (S.D.) for ISACA Members (n = 337)
Collection	5.28 (1.19)	5.11 (1.04)	5.45 (1.16)
Errors	5.36 (1.06)	5.57 (.99)	5.46 (1.11)
Unauthorized Secondary Use	5.77 (1.22)	5.74 (1.14)	6.15 (1.07)
Improper Access	6.10 (.89)	5.83 (1.01)	5.90 (1.01)
OVERALL	5.63 (.78)	5.56 (.83)	5.74 (.86)

Larger means are associated with higher levels of concern (see Table 1.).

tional information privacy practices" construct. Both of these assessments appear to be consistent with the majority views of scholars, consumers, and advocates, and the four-dimension model of the construct seems to reflect current thinking. We acknowledge, however, that this dimensionality is neither absolute nor static, since perceptions of advocates, consumers, and scholars could shift over time. Thus, the instrument should be viewed as measuring the *most central* dimensions of the construct at this time. Future research endeavors might consider any changes in these dimensions that may occur.

Second, while we made a concerted effort to validate the instrument in a nomological model of antecedents, individual personality variables, privacy concerns, and future behavioral intentions (Stage 3), it should be noted that this nomological model is not purported to be an exhaustive one, nor did we test it in an experimental, causal context. Indeed, theories regarding the interrelationships between privacy concerns and other constructs are not fully developed in the literature at present, and the creation of a full model is a task appropriate for a subsequent study. Furthermore, because of the constraints of time and length associated with administration of written surveys, we were unable to test all the antecedents, personality variables, and behavioral intentions with a single sample. Despite these limitations, this work has significant implications for both researchers and managers. We examine each in the following sections.

Implications for researchers

Like many other areas within the IS domain, little attention has been paid to instrumentation issues in privacy research. Now, with a validated instrument for measuring individuals' concerns about organizational information privacy practices, researchers can undertake studies to carefully examine the links between relevant privacy-related variables, privacy concerns, and outcomes of those concerns.

Theoretical models (see Stone and Stone, 1990) often posit theoretical relationships that include privacy concern as one of the model's constructs. With respect to *factors that may impact levels of concern*, it has been suggested that concerns may be context-sensitive based on either the type of information being managed (Culnan, 1993; Stone and Stone, 1990) or the type of organization collecting and storing the data (Stone, et al., 1983). Concerns may also be associated with numerous personality factors and demographic data (see review in Stone and Stone, 1990). Further, some public opinion survey findings (Equifax, 1990) suggest that levels of concern on some subscales may be lower for professionals with day-to-day exposure to information processing activities.

There may also be *factors that are impacted by levels of concern*. It has been asserted that individuals may take a variety of different actions based on their levels of concern, such as "opting out" of various activities (Culnan, 1993; Stone and Stone, 1990). Furthermore, perceptions of organizational privacy policies and practices may be related to levels of employee concern (Smith, et al., 1995), and levels of concern may also be associated with different cultural values and regulatory structures in various countries (Milberg, et al., 1995). It is clear that a significant research stream could emerge from empirical tests of the relationships between the antecedents, associated factors, levels of concern, and outcomes.

As suggested by the discussion in the previous paragraph, most of this instrument's usefulness will come from its application in positivist research—in particular, the development and testing of theories that take the form of independent and dependent variables (Lee, 1991). But the instrument may also assist a researcher in conducting interpretive research on what the meaning of information privacy is for the individuals themselves in an organization, apart from or prior to whatever a positivist theory would define it to be (Lee, 1991). Full understanding of a phenomenon is best achieved not through any singularity in approach, but rather, through iterative cycles

of positivist and interpretive research (Lee, 1991).[23] To the extent that researchers confirm some of the theoretical linkages in positivist approaches (e.g., by showing that individuals exhibit higher levels of concern when stimulus materials prompt them to think about medical data rather than financial data), these findings may then feed back to interpretive studies (e.g., field studies that examine different approaches to managing medical data and managers' perceptions of differing responsibility levels).

As privacy increases in importance, it behooves the IS research community to carefully consider the complexity of individuals' concerns, the factors that may cause increased levels of concern, and the outcomes of those concerns. The instrument developed in this study should enable future work in this important area.

Implications for managers

This study, which identified the most central dimensions of individuals' concerns about organizational information privacy practices, can serve as the first step on a path of proactive management. By carefully considering their own organizations' approaches to the four major dimensions of concern—Collection, Errors, Unauthorized Secondary Use, and Improper Access—managers can identify underlying problems and take corrective actions as appropriate. Table 10 contains a set of possible recommendations that might be embraced for each of the dimensions.

As an example, IS professionals can address secondary use issues by identifying the secondary uses of data within their organizations and ensuring that the appropriate technological approaches are being adopted for tracking purposes. It is acknowledged that IS managers and executives will seldom be in a position to unilaterally correct all the organizational problems in these domains since they are likely to involve some degree of existing organizational policy. Changing existing policy will demand attention from general managers at a senior level. However, IS professionals can be aggressive in challenging organizational policies for sharing personal data with outside organizations, and they may insist on tighter interpretations of the "need to know" when organizational policies regarding access are constructed.

By taking a proactive stance in managing these dimensions of concern, IS managers and executives may reduce the probability that onerous regulatory options will be pursued (see Milberg, et al., 1995; Smith, 1994). Research has shown that increased concerns about information privacy are associated with increased levels of governmental involvement in organizational privacy management (Milberg, et al., 1995), but so far, managers have been primarily reactive in addressing information privacy concerns (Smith, 1994). Managers should be alert to the value-laden choices that are made by systems designers and implementers (Kling, 1978; Mowshowitz, 1976), because these choices can ultimately impact the privacy domain and reactions thereto. This study, along with future research addressing the antecedents and consequences of various concerns, may allow managers to evaluate specific situational contexts and manage responses to information management practices, thus avoiding costly consumer and/or regulatory backlashes.

Acknowledgements

The three authors contributed equally on this research. We gratefully acknowledge several individuals for their assistance in administering versions of the survey instrument: Tom Cooke, Elizabeth Cooper-Martin, Mary Culnan, Bill DeLone, Mark Keil, Mike McCarthy, Keri Pearlson, Craig Smith, Bob Thomas, Suzie

[23] Of course, the choice of research approach(es) is highly contextual and depends on the type of research question being asked (Yin, 1988), the findings from previous studies (Bonoma, 1985), and the levels of understanding regarding the phenomenon of interest (Lee, 1991). See Bonoma (1985), Lee (1991), Orlikowski and Baroudi (1991), and Yin (1988) for a broad discussion of the relationships between research approaches.

Table 10. Recommendations to IS Community

Area of Concern	Recommended Actions Within IS Domain	Recommended Actions in Broader Organizational Domain
Improper Access	• Implement technological controls on access to systems • Ensure that applications are designed so that access can be restricted to narrowest domains possible	• Lobby for organizational access policies with a tight definition of "need to know" • Challenge liberal interpretations of "need to know"
Unauthorized Secondary Use	• Ensure that all internal uses of personal data can be tracked • Refuse to release personal data to outside entities without explicit senior management approval	• Lobby for clear organizational policies on "intended use" for personal data • Challenge internal uses of personal data that are outside "intended use" boundaries • Lobby for organizational policies restricting outside sharing of personal data
Errors	• Ensure that applications are designed with appropriate edit techniques	• Identify tradeoffs regarding error controls to senior management; ensure informed decision making
Collection	• Practice parsimonious database design	• Challenge excessive collection of personal data within organization • Lobby for organizational policy that limits data collection to minimal levels required for business

Weisband, and Berry Wilson. We also acknowledge with gratitude the organizations that supported this survey research, including an anonymous bank, two anonymous insurance organizations, an anonymous credit card issuer, the Information Systems Audit and Control Association (ISACA), and the Georgetown University Center for Business-Government Relations. Ernest Kallman is especially acknowledged for his assistance in much of the data collection. We also appreciate the data entry help provided by Emmy Curtis, Debra Miller, and Shirmel Richards. Mary Culnan provided helpful comments on an earlier version of this paper. We also gratefully acknowledge the senior editor, associate editor, and five anonymous referees for their insightful comments on an earlier draft.

References

ACM (Association for Computing Machinery). "Code of Ethics," *Communications of the ACM* (23:7), July 1980, p. 425.

Bagozzi, R. P. *Causal Modeling in Marketing*, John Wiley and Sons, New York, 1980.

Bagozzi, R. P. "An Examination of the Validity of Two Models of Attitude," *Multivariate Behavioral Research*, July 1981, pp. 323-359.

Bagozzi, R. P. "A Holistic Methodology for Modeling Consumer Response to Innovation," *Operations Research*, January-February 1983, pp. 128-176.

Bagozzi, R.P. "Assessing Construct Validity in Personality Research: Applications to Measures of Self-Esteem," *Journal of Research in Personality* (27:1), March 1993, pp. 49-87.

Bagozzi, R. P. and Phillips, L. W. "Representing and Testing Organizational Theories: A Holistic Construal," *Administrative Science Quarterly* (27:3), 1982, pp. 459-489.

Bagozzi, R. P. and Yi, Y. "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science* (16), Spring 1988.

Bagozzi, R. P. and Yi, Y. "Multitrait-Multimethod Matrices in Consumer Research," *Journal of Consumer Research* (17:4), March 1991, pp. 426-439.

Barki, H. and Hartwick, J. "Measuring User Participation, User Involvement, and User Attitude," *MIS Quarterly* (18:1), March 1994, pp. 59-82.

Bearden, W. O., Netemeyer, R. G. and Mobley, M. F. *Handbook of Marketing Scales*, Sage Publications, Newbury Park, CA, 1993, pp. 3-8.

Bennett, C. J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca, NY, 1992.

Bentler, P. M. "Comparative Fit Indexes in Structural Models," *Psychological Bulletin* (107:2), 1990, pp. 238-246.

Bentler, P. M. and Bonett, D. "Significance Tests and Goodness of Fit in the Analysis of Covariance Structures," *Psychological Bulletin* (88:3), November 1980, pp. 588-606.

Berscheid, E. "Privacy: A Hidden Variable in Experimental Social Psychology," *Journal of Social Issues* (33:3), 1977, pp. 85-101.

Bonoma, T. V. "Case Research in Marketing: Opportunities, Problems, and a Process," *Journal of Marketing Research* (XXII), May 1985, pp. 199-208.

Cambridge Reports. "Technology and Consumers: Jobs, Education, Privacy," Bulletin on Consumer Opinion no. 157, Cambridge, MA 1989.

Campbell, D. T. and Fiske, D. W. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56:2), March 1959, pp. 81-105.

Cespedes, F. V. and Smith, H. J. "Database Marketing: New Rules for Policy and Practice," *Sloan Management Review* (34), Summer 1993, pp. 7-22.

Churchill, G. "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research* (XVI), February 1979, pp. 64-73.

Cook, T.D. and Campbell, D. T. *Quasi-experimentation: Design and Analysis Issues for Field Settings*, Rand McNally, Chicago, 1979.

Cote, J. A. and Buckley, M. R. "Measurement Error and Theory Testing in Consumer Research: An Illustration of the Importance of Construct Validation" *Journal of Consumer Research* (14), March 1987, pp. 579-582.

Cozby, P.C. "Self-disclosure: A Literature Review," *Psychological Bulletin* (79:2), February 1973, pp. 73-91.

Cronbach, L. "Test Validation" in *Educational Measurement* (2nd edition), R. L. Thorndike (ed.), American Council on Education, Washington, D.C., 1971, pp. 443-507.

Cronbach, L. J. and Meehl, P. E. "Construct Validity in Psychological Tests," *Psychological Bulletin* (52:4), July 1955, pp. 281-302.

Culnan, M. J. "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (17:3), September 1993, pp. 341-363.

Cyert, R. M. and March, J. G. *A Behavioral Theory of the Firm*, Prentice Hall, New York, 1963.

Date, C.J. *An Introduction to Database Systems* (4th ed.), Addison-Wesley Publishing Company, Reading, MA, 1986.

Equifax Inc. *The Equifax Report on Consumers in the Information Age, 1990. Also Harris-Equifax Consumer Privacy Survey 1991, Harris-Equifax Consumer Privacy Survey 1992,* and *Harris-Equifax Health Information Privacy Survey 1993.* Equifax Inc., Atlanta, GA.

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

Fornell, C. and Larcker, D. F. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18), February 1981, pp. 39-50.

Gordon, M.E., Slade, L.A., and Schmitt, N. "The 'Science of the Sophomore' Revisited: From Conjecture to Empiricism," *Academy of Management Review* (11:1), 1986, pp. 191-207.

HEW (U.S. Department of Health, Education, and Welfare). *Records, Computers, and the Rights of Citizens: Report of the Secretary's*

Advisory Committee on Automated Personal Data Systems, U.S. Government Printing Office, Washington, D.C., 1973.

Jarvenpaa, S. L., Dickson, G. W., and DeSanctis, G. "Methodological Issues in Experimental IS Research: Experiences and Recommendations," *MIS Quarterly* (9:2), June 1985, pp. 141-156.

Jessor, R. and Jessor, S. *Problem Behavior and Psychosocial Development*, Academic Press, New York, 1977, pp. 234-235, as reproduced in Measures of Personality and Social Psychological Attitudes, J. P. Robinson, P. R. Shaver, and L. S. Wrightsman (eds.), Academic Press, San Diego, 1991, pp. 355-358.

Joreskog, K. and Sorbom, D. *LISREL VI: Analysis of Linear Structural Relationships by the Maximum Likelihood and Least Squares Methods*, Scientific Software, Mooresville, IN, 1984.

Katz, J. E. and Tassone, A. R. "Public Opinion Trends: Privacy and Information Technology," *Public Opinion Quarterly* (54), Spring 1990, pp. 125-143.

Kelvin, P. "A Socio-psychological Examination of Privacy," *British Journal of Social Clinical Psychology* (12:3), September 1973, pp. 248-261.

Kerlinger, F. N. *Foundations of Behavioral Research* (3rd ed.), Holt, Rinehart, and Winston, New York, 1986, pp. 477-483.

Kling, R. "Value Conflicts and Social Choices in Electronic Funds Transfer Systems Developments," *Communications of the ACM* (21:8), August 1978, pp. 642-657.

Ladd, J. "Computer and Moral Responsibility: A Framework for Ethical Analysis," in *The Information Web: Ethical and Social Implications of Computer Networking*, C. Gould (ed.), Westview Press, Boulder, CO, 1989.

Laudon, K.C. Dossier Society: *Value Choices in the Design of National Information Systems*, Columbia University Press, New York, 1986.

Laufer, R.S. and Wolfe, M. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), 1977, pp. 22-41.

Lee, A. S. "Integrating Positivist and Interpretive Approaches to Organizational Research," *Organizational Science* (2:4), 1991, pp. 342-365.

Levin, H.A. and Askin, F. "Privacy in the Courts: Law and Social Reality," *Journal of Social Issues* (33:3), 1977, pp. 138-153.

Linowes, D. F. *Privacy in America: Is Your Private Life in the Public Eye?* University of Illinois Press, Urbana, IL, 1989.

Mason, R. O. "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), March 1986, pp. 4-12.

McDonald, R. P. and Marsh, H. W. "Choosing a Multivariate Model: Noncentrality and Goodness of Fit," *Psychological Bulletin* (107:2), March 1990, pp. 247-255.

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. "Values, Personal Information Privacy Concerns, and Regulatory Approaches," *Communications of the ACM* (38:12), December 1995, pp. 65-74.

Miller, A. "Computers and Privacy," in *Ethics and the Management of Computer Technology*, W. M. Hoffman, and J. M. Moore (eds.), Oelgeschlager, Gunn, and Hain Publishers, Inc., Cambridge, MA, 1982.

Mowshowitz, A. *The Conquest of Will*, Addison-Wesley, Reading, MA, 1976.

Orlikowski, W. J. and Baroudi, J. J. "Studying Information Technology in Organizations: Research Approaches and Assumptions," *Information Systems Research* (2:1), 1991, pp. 1-28.

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

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

Smith, H. J., Milberg, S. J., and Kallman, E. A. "Privacy Practices Around the World: An Empirical Study," working paper, Georgetown University, Washington, D.C., 1995.

Stone, D. L. "Relationship Between Introversion/Extraversion, Values Regarding Control Over Information, and Perceptions of Invasion of Privacy," *Perceptual and Motor Skills* (62:2), April, 1986, pp. 371-376.

Stone, E. F. and Stone, D. L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," in *Research in Personnel and Human Resources Management* (8), K. M. Rowland and G. R. Ferris (eds.), JAI Press, Greenwich, CT, 1990, pp. 349-411.

Stone, E. F., Gardner, D. G., Gueutal, H. G., and McClure, S. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology* (68:3), August 1983, pp. 459-468.

Straub, D. W. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), June 1989, pp. 146-169.

Straub, D. W., Jr. and Collins, R. W. "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly* (14:2), June 1990, pp. 142-156.

Straub, D.W., Limayem, M., and Karahanna, E. "Measuring System Usage: Implications for IS Theory Testing," *Management Science* (41:8), August 1995, pp. 1328-1342.

Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W., and Fromkin, H.L. "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology* (66:3), June 1981, pp. 308-313.

Warren, C. and Laslett, B. "Privacy and Secrecy: A Conceptual Comparison," *Journal of Social Issues* (33:3), 1977, pp. 43-51.

Westin, A. F. *Privacy and Freedom*, Atheneum Publishers, New York, 1967.

Westin, A.F. "Consumer Privacy Issues in the Nineties," in *The Equifax Report on Consumers in the Information Age*, Equifax Inc., Atlanta, GA, 1990, pp. XVIII-XXVIII.

Westin, A. F. and Baker, M. A. *Databanks in a Free Society*, Quadrangle Books, New York, 1972.

Yin, R. K. *Case Study Research: Design and Methods*, Sage Publications, Beverly Hills, CA, 1988.

About the Authors

H. Jeff Smith is associate professor, School of Business, Georgetown University, Washington, D.C. He holds B.S. degrees in computer science and mathematics from North Carolina State University; an M.B.A. degree from the University of North Carolina at Chapel Hill; and a D.B.A. degree from Harvard University. His research focuses on the social issues created by the use of emerging technologies. His research has been published in *Communications of the ACM* and *Sloan Management Review*. He is the author of *Managing Privacy: Information Technology and Corporate America*, published by the University of North Carolina Press.

Sandra J. Milberg is assistant professor, School of Business, Georgetown University, Washington, D.C. She holds a B.A. degree in sociology from Washington University, St. Louis; an M.S. degree in marketing from Carnegie Mellon University, Pittsburgh; and a Ph.D. degree in business administration from the University of Pittsburgh. Her research focuses on consumer privacy issues, brand equity, and the roles of affect and cognition in attitude formation and choice behavior. Her research has been published in *Communications of the ACM*, *Journal of Consumer Research*, *Journal of Personality and Social Psychology*, and *Journal of Experimental Social Psychology*.

Sandra J. Burke is assistant professor, School of Business, Georgetown University, Washington, D.C. She holds a B.A. degree in economics from Michigan State University, and M.B.A and Ph.D. degrees in marketing from The University of Michigan. Her research focuses on ethical/privacy issues in marketing, consumer information processing and decision making, and consumer inference use and formation. Her research has been published in *Communications of the ACM*, *Advances in Consumer Research*, and *Journal of Behavioral Decision Making*.

Appendix

Confirmatory Factor Analysis

Because an *a priori* hypothesis is tested, CFA has several advantages over traditional methods of scale validation (Bagozzi, 1983). CFA (1) provides explicit measures to assess construct validity and to correct for the unreliability of measures that can contaminate theoretical relations, (2) represents explicitly the extent of measurement error, and (3) overcomes the fundamental indeterminacy (problem of non-unique solutions) of exploratory factor analysis. To be more specific, in models where sequences of relationships occur, it is important to explicitly represent and control for systematic and random errors in measurement. Failure to do so can lead to biased and inconsistent estimates of parameters. Furthermore, most procedures that employ the measurements obtained from scale administrations (e.g., correlations, regression, ANOVA) implicitly assume the absence of random and systematic errors in observations. Yet, when Cote and Buckley (1987) applied CFA techniques to 70 published data sets, they found that measurement error, on average, accounted for 32 percent of total variance. CFA goes beyond traditional validation methods, in that theoretical concepts, non-observational hypotheses, and errors are explicitly assessed.

Furthermore, while oblique or orthogonal exploratory factor analyses are traditionally used in scale validation, neither procedure yields a unique solution in a statistical sense. Once a set of factors is found, an infinite number of other equally acceptable factors can be formed as non-singular linear transformations of the first set (Bagozzi, 1983). Again, if the researcher attempts to interpret the factors, use the loadings for further analysis, or compute scores to test hypotheses, this implicit non-uniqueness can cause problems. CFA yields a unique solution on an *a priori* basis. A researcher hypothesizes a model and then tests the goodness-of-fit of the model on a particular set of data. In addition, CFA is used to assess the overall fit of this model versus the fit with other models reflecting alternative underlying structures of this construct to assess validity.