December 2004

Addressing End-User Privacy Concerns

Julia Earp
North Carolina State University

Annie Anton
North Carolina State University

Addressing End-User Privacy Concerns

Julia B. Earp
North Carolina State University
Julia_Earp@ncsu.edu

Annie I. Antón
North Carolina State University
e-mail address

ABSTRACT

Organizations engaged in electronic transactions have a social, and often legal, responsibility to adopt and disclose a policy for protecting customer information. Guidelines for establishing an organizational privacy policy frequently emphasize the inclusion of the fair information practice (FIP) principles that were established in 1973. The increasingly diverse population of Internet users suggests that a different approach to privacy policies may be required. Understanding users' privacy expectations can improve the creation of effective privacy policies and practices. In this paper, we examine which aspects of the FIPs address, or do not address, consumers' fundamental privacy expectations. This exploration is based on a survey of over 1,000 Internet users having a diverse range of Internet experience. We also explore the different views held by novice Web users and experienced Web users, and relate this relationship to privacy policy development.

Keywords

Privacy management, information privacy, privacy policy.

INTRODUCTION

Information privacy has been recognized as an important concern in management, and its significance will continue to escalate as the value of information continues to grow (Mason, 1986; Raul, 2002; Rust, Kannan, & Peng, 2002). Understanding and protecting personal privacy in information systems is becoming even more critical with the widespread use of networked systems and the Internet, which provide opportunities to collect large amounts of personal information about online users, potentially violating those users' personal privacy (Belotti, 1997; Clarke, 1999). Additionally, the increasingly diverse population of Internet users is introducing new challenges about how organizations should communicate privacy practices to its customers. Despite growing concerns with information privacy, the design of technologies often leaves privacy as something that is considered and addressed as an afterthought (Antón & Earp, 2001). Organizations have played catch-up by developing privacy policy statements, but these have been criticized as being either feeble or too complex and convoluted for readers to understand (Antón, et al., 2004; Kasanoff, 2002).

The business interest in privacy management is that organizations need consumers to feel comfortable disclosing personal information required for legitimate business activities such as relationship marketing. It is important for organizations to provide consumers with a privacy policy that outlines organizational privacy practices in such a way that the consumer understands the benefits of disclosure while receiving assurance that such disclosure produces low personal risk. Privacy policies are typically created by managers, legal professionals or information systems professionals. Although there is no precise approach for determining what information should be presented in a privacy policy or how it should be written, the accepted norm revolves around the inclusion of fair information practices that are adhered to by the organization. This is an admirable approach, and a good foundation, but what about organizations that engage in fair information practices that seem disconcerting to some consumers? Consider a website that allows partnering third parties to collect customer information (e.g. pages visited) through Web bugs. Since the website organization is not collecting the information, fair information practices do not oblige the website to inform the consumer of that practice. However, many consumers would cringe if they were aware of that website's practice of allowing third party Web bugs. Rather than simply advocating the disclosure of fair information practices, it may be more constructive to consider a larger set of information practices. More importantly, it may benefit Internet consumers if we focus on something besides privacy policy content. In this paper, we propose additional considerations that go beyond privacy policies. We base this recommendation on survey data of over 1000 consumers that depicts who Internet consumers are and what concerns them with regard to information use.

Ideally, website privacy policies should address users' concerns about privacy -- but this may or may not be the case. There is a gap in the literature pertaining to research that relates user concerns with website privacy policy creation. We address that omission by using survey data to assess user privacy concerns as they relate to privacy policy disclosures of fair information practices

BACKGROUND

In the 1970s, the United States Congress held hearings in which privacy advocates sought to outlaw the use of centralized computer databases by credit bureaus. These hearings lead to the recognition that organizations have certain responsibilities and individuals have certain rights in terms of information collection and use. Since 1973, the Fair Information Practice (FIP) Principles (The Code of Fair Information Practices, 1973) have served as the basis for evaluating and establishing the policies and rules that underlie most privacy laws and practices in the United States. The FIPs aim to balance the privacy interests with legitimate business needs of collecting customer information. The FIP Principles consist of the following (The Code of Fair Information Practices, 1973):

- notice/awareness – Consumers should be given notice of an organization's information practices before any personal information is collected from them;
- choice/consent – Consumers should be given options as to how any personal information collected from them may be used;
- access/participation – Individuals must be given the ability to access data about him or herself and to contest that data's accuracy and completeness;
- integrity/security – Reasonable steps must be taken to ensure data is accurate and secure;
- enforcement/redress – A mechanism must be in place to enforce the four core principles of privacy listed above.

Although organizations engaged in electronic transactions should disclose privacy policies that are based on the FIPs (The Code of Fair Information Practices, 1973; FTC, 1998; FTC, 2000), several studies (Antón, Earp and Reese, 2002; Culnan, 1999; EPIC, 1999) have found that Internet privacy policies do not always reflect fair information practices. The U.S. FIP Principles reflect a subset of the 1980 OECD guidelines that characterize the current global standard for privacy protection and serve as a basis for legislation in OECD member countries. In particular, the OECD guidelines were developed to uphold human rights while concurrently preventing interruptions in international flows of data (OECD, 1980).

Some organizations rely on web privacy seals to help communicate trust to consumers. These web seal programs require participating organizations to post specific information regarding privacy practices. For example, one of the most common privacy seal programs, TRUSTe, requires organizations to disclose the following information in their online privacy policies (see http://www.truste.com/programs/pub_principles.html):

- What personal information is being gathered by the site;
- Who is collecting the information;
- How the information will be used;
- With whom the information will be shared;
- The choices available to users regarding collection, use, and distribution of their information;
- The security procedures in place to protect users' collected information from loss misuse, or alteration; and
- How users can update or correct inaccuracies in their pertinent information.

That information reflects the same information described in the FIPs.

In recent surveys of user attitudes pertaining to the Internet (Cranor, et al., 2000; Harris, 1991, 1994, 1996, 1998), privacy has been consistently rated as one of the most important concerns by users engaging in online transactions. In particular, security and privacy of business-to-user websites are the most influential dimensions of on-line users' purchase intent (Ranganathan.

& Ganapathy, 2002). Internet users are a primary factor in the growth of online commerce, therefore, it is important to appropriately align policies and practices of the e-commerce system with these users' needs and concerns (Antón, Earp & Carter, 2002). Simply addressing the FIPs may provide an organization the opportunity to omit important information. The attitudes and concerns of online users have been the focus of several recent studies (Earp, et al., 2003; Cranor, et al., 2000; FTC, 1998, 2000; Smith, Milberg, & Burke, 1996), but those studies do not explore user concerns in relation to Internet privacy policy content. It is important for information systems managers to relate website privacy policies to user concerns, so these managers can plan and direct systems to meet those concerns. This is especially imperative considering the influence that user trust can have on e-business success (Jones, Wilikens, Morris, & Masera, 2000).

Ackerman, Cranor, and Reagle (1999) surveyed 381 United States Internet users about their online privacy concerns regarding specific online scenarios. Based on their data, these researchers proposed three categories of Internet users. The *Privacy Fundamentalists* are individuals who are extremely concerned about their privacy; they rarely reveal any private information about themselves, even when privacy protection measures are in place. The *Pragmatic Majority*, as the name suggests, represents the bulk of Internet users; they are individuals who are concerned about privacy, but less so than the Privacy Fundamentalists. The Pragmatic Majority often has specific concerns that can be addressed by making privacy policies available to them. The *Marginally Concerned* refers to those individuals who are willing to provide personal information to websites under almost any circumstances.

The three most influential factors of user confidence as found in a recent Internet privacy survey were (in order of most to least influential): the company name, providing users the option to "opt-out" of data collection, and the presence of a site privacy policy (Earp and Baumer, 2003). Fifty-four percent of respondents surveyed in this study said they would read a website's privacy policy on the first visit, and 66% of respondents indicated increased confidence in a website if a privacy policy was present. Although the organization's brand name is the most influential characteristic, the presence of an appropriate privacy policy can benefit those websites that do not have a well-recognized brand name.

A recent study (Liu and Arnett, 2002) found that 51.7% of Fortune 500 companies provide a website privacy policy. Of these privacy policies 26.5% address access/participation, 45.9% address security/integrity, 46.7% address choice/consent and 92.2% address notice/awareness. The main features of these Fortune 500 privacy policies include: information use, collection, disclosure, contact, opt-out, security, cookie, link warning, access/correction, internal protection, children protection, and policy consent.

Rather than assuming that privacy policies would be focused on the Fair Information Practice principles (FTC 1998, 2000), a recent content analysis of such policies was performed (Antón, Earp and Reese, 2002) to determine what website privacy policies actually say. The content analysis resulted in a taxonomy of web policy statements: notice/awareness, choice/consent, access/participation, integrity/security, enforcement/redress, information monitoring, information aggregation, information storage, information transfer, information collection, information personalization, contact. After developing the taxonomy the researchers then categorized the content of 23 website privacy policies. They found that privacy policies most often discuss, from most frequent to least frequent: (1) Integrity/Security, or goals assuring security about collected data, (2) Collection, or goals about how data are collected – either by direct entry of user, or by unobservable means such as using browser cookies; and (3) Choice/Consent, or goals about having the user be able to decide what information can be used about them.

The next section of this paper discusses our research approach to discovering what Internet users are most concerned about with regard to privacy policies.

METHODOLOGY

Developing a Survey Instrument to Measure Users Privacy Concerns

A web-based survey approach was deemed the most appropriate means for data collection to accomplish the objectives of this study since the population of interest is comprised of general Internet users. In this section, we provide a brief overview of the survey measurement items and our pilot study.

Measurement Items

To measure user privacy concerns the measurement items were based upon the 12 privacy protection goal and vulnerability classes described in (Antón and Earp, 2004). Following a careful item development process, as suggested by Nunnally (Nunnally, 1978), 60 items were created by the development team. These items were reviewed by survey experts and a panel of privacy experts. These experts reviewed the items for clarity, and to ensure that they accurately represented the concepts being measured for content validity of the scale items. The survey items were then given to a focus group of 26 Internet users to evaluate the items for their applicability to the respective privacy category. Items that were determined to be inconsistent were either eliminated or revised, resulting in 37 items that addressed user privacy concerns.

Pilot Testing

We pilot tested the survey with a sample of 386 students from a large southeastern university. Of these, 347 respondents returned usable surveys. Small amounts of missing data were replaced with the mean of that item (Roth, Switzer and Switzer, 1999). Exploratory factor analysis and Cronbach's alphas, representing inter-item reliability, provided tentative support for the privacy classes with respect to user privacy concerns. Three factors emerged and 31 items loaded cleanly. Based on additional exploratory analysis and Nunnally's reliability heuristics (Nunnally, 1978), we reworded some of the items, resulting in a revised survey instrument having 36 scale items pertaining to the privacy taxonomy categories in addition to open-ended, demographic, familiarity and usage items.

Survey Distribution

The revised survey was distributed online to Internet users worldwide. During the one month time period, 1,525 responses were collected. Out of these responses, 80 were missing 20% or more of the data and 440 were completely null. Our analysis is based on the resulting 1,005 usable surveys. Because privacy is more of a concern with transaction-based websites, it is important to note that 608 (65%) respondents had made an online purchase within the past 30 days. Respondents represented 30 countries with 88% being from the United States.

Exploratory Factor Analysis

A randomly selected subset (n=360) of the 1,005 usable records was employed for factor analysis. Those items that loaded less than 0.40 or cross-loaded were discarded. This analysis resulted in six factors: *Personalization, Collection, Transfer, Notice/Awareness, Storage,* and *Access/Participation.* Items were combined additively to form measures. Table 3 shows descriptive statistics, as well as reliabilities for these measures. Reliabilities range from 0.74 (Access/Participation) to 0.89 (Transfer). The factor correlation matrix (see Table 1), indicated discrimination between these constructs. Two factors, collection and personalization, were more highly correlated (0.60) than others, although they did factor cleanly.

	Mean	*s.d.*	*1*	*2*	*3*	*4*	*5*	*6*
1. Collection	3.96	1.24	(0.87)					
2. Personalization	3.47	1.26	0.620	(0.83)				
3. Notice/Awareness	4.68	0.62	0.309	0.280	(0.82)			
4. Transfer	4.78	0.57	0.329	0.370	0.410	(0.89)		
5. Storage	4.56	0.78	0.333	0.321	0.414	0.43	(0.82)	
6. Access/Participation	4.36	0.98	0.087	0.026	0.221	0.18	0.16	(0.74)

Table 1. Descriptive Statistics and Correlations (Coefficient Alphas are on the Diagonal)

Confirmatory Factor Analysis

We compared the six-factor model based on the resulting factors of the pilot study to a two-factor model based on the privacy taxonomy's two super classes (protection and vulnerability). We did not use any data that had been used in the exploratory analysis. The overall fit of the six-factor model was analyzed as follows. The chi-square values for the comparative models suggest the six-factor model is a more adequate fit (six factor chi-square of 390.17 with 194 degrees of freedom, compared to the two factor chi-square of 1502.18 and 208 degrees of freedom). RMSEA also supports the six-factor model over the two-factor model (six factor RMSEA = 0.063; two factor RMSEA = .18).

CFI provides a measure of complete covariation in the data; therefore, values greater than 0.90 indicate an acceptable fit to the data (Bentler, 1990). NNFI considers the complexity of the model when comparing the hypothesized model with another model. Like the CFI, it is desirable to have a NNFI greater than 0.90. These measures continue to support the six-factor model (six factor CFI = .94; two factor CFI = .58; while six factor NNFI = .92; two factor NNFI = .53). According to the standardized RMR statistic, the six-factor model represents a fairly good fit (RMR = .069) while the two-factor model represents a poor fit (RMR = .11). The exploratory and confirmatory analyses were convincing that we had a good measure for our research question about what is really what Internet users are concerned about regarding privacy policies.

RESULTS AND DISCUSSION

The survey data reveals that Internet users are most concerned with privacy issues regarding: (1) transfer, or concerns that their data will be shared, lent, or sold to other entities (mean = 4.78, stdev = 0.58), (2) notice / awareness, or concerns about having full information from the organization about how their data might be used, before they hand any over (mean = 4.67, stdev = 0.66), and (3) storage, or how the organization intends to store and maintain the user data (mean = 4.56, stdev = 0.78). The notice/awareness principle dictates that consumers should be given notice of an organization's information practices before any personal information is collected from them. Such notice could include details regarding the organization's information transfer practices, however, in many cases consumers may not realize that they were given such notice. Consider the 40 online financial privacy policies analyzed in (A, E, B, H, J, S 2004) where the Flesch Grade Level (FGL) was calculated for each policy. The FGL determines the U.S. grade-school equivalency level of a text and is also based on the average number of syllables and sentence length. In other words, text having an FGL value of 14 means a person with less than 14 years of education (i.e., 2 years of college) would encounter difficulties while attempting to read the text. Of the 40 analyzed privacy policies, FGL values ranged from 10.42 to 18.72. The average education of the Internet population over age 25 is 14.4 years [NTI02]. These statistics indicate that many consumers may not be capable of interpreting information regarding an organization's privacy practices. In such instances, consumers will not be aware of the organization's privacy practices even though the organization abided by the FIPs and provided formal notice via a privacy policy.

A second way to segment the population of Internet users according to level of Web experience: novice Web users and experienced Web users. For purposes of this discussion, we define experienced Web users and novice Web users as follows. Experienced users are those who began using the Web over 4 years ago, use the Web at least 10 hours per week, recognize when a website is secure (e.g. Internet Explorer's lock icon), and use a second email address (e.g. hotmail.com address) to keep a primary email address private. Novice users are all other Web users. We received 1005 usable responses and 253 (25%) of these were categorized as experienced users while 752 (75%) of them were categorized as novice users.

Table 2 shows demographics of the two groups, novice and experienced Web users. Interestingly, 23% of the novice users answered the gender item with either "rather not say" or did not respond at all. Only 2% of the experienced users answered with either "rather not say" or did not respond at all. Similarly, 20% of novice users answered the age item with either "rather not say" or did not respond at all. None of the experienced users answered with either "rather not say" or did not respond at all. The survey was an anonymous survey and did not request any personally identifiable information from the respondents; therefore, requesting respondent age and gender should not have raised any concerns. This implies that the experienced Web users are more educated about circumstances that warrant legitimate privacy concerns and those that do not. It is likely that novice users do not understand exactly what kinds of information in cyberspace equate to personally identifiable information that should be closely guarded. Similarly, they probably do not understand how websites can collect personally identifiable information or even legally transfer it to a third party.

Table 3 shows the survey items that generated a p-value < 0.01 when comparing novice Web users with experienced Web users. Aside from item Q18, novice users agreed more strongly with the statements in Table 3. This illustrates the level of confusion that novice users experience. Consumer privacy on the Internet is more threatened by the transfer of information to and from third parties. When a consumer reveals information about his or herself, that consumer expects to receive a desired service or product. Anything beyond that may be viewed as unnecessary or simply annoying. Expert Web users are more tolerant of common techniques of data collection while simply browsing — possibly because they understand the harmless nature and necessity of some of these techniques. For example, websites frequently collect information about a user's browser application to optimize the website's appearance to the user. Expert users may be aware that some websites appear different depending on the browser being used to display the website. This is a concept that novice Internet users may be unaware of, and as a result, do not understand why a website would collect such information about a user's computer.

Items Q21, Q22 and Q23 (see Table 3) represent collection items. This implies that novices don't really understand the collection of these things from a privacy standpoint nor do they understand the nature of what is being collected — perhaps because those items do not refer to personally identifiable information.

	Novice	Experienced
Gender		
Males	435	187
Females	217	62
Rather Not Say	21	4
No Response	79	0
Age		
15 – 21	54	25
22 – 28	147	92
29 – 35	136	66
36 – 42	111	34
43 – 49	71	16
50 – 57	78	16
57 +	65	4
Rather Not Say	21	0
No Response	69	0

Table 2. Demographics of Novice and Experienced Web Users

Survey Item	P-Value
Q18: I want to be able to disallow (opt-out) services that consolidate my PII with my other information that is kept by different sources.	0.003
Q21: I mind when a Web site that I visit collects (without my consent) information about my browser information.	0.0002
Q22: I mind when a Web site that I visit collects (without my consent) information about my IP address (a number that uniquely identifies your computer from all other computers on the Internet).	0.0003
Q23: I mind when a Web site that I visit collects (without my consent) information about the type of computer/Operating System I use.	0.0074
Q27: I mind when a Web site uses my (PII) to customize my browsing experience.	0.0065
Q28: I mind when a web site uses cookies to customize my browsing experience. (A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time).	0.0001
Q29: I mind when a Web site uses my purchasing history to personalize my browsing experience (e.g. by suggesting products for me to purchase).	0.0065
Q34: I am concerned about unauthorized hackers getting access to my information.	0.0009

Table 3. Survey Items with p<0.01 (Novice vs. Experienced Users)

Table 4 shows what users are concerned about in order from most concerned to less concerned. Although the sample of 1005 users were most concerned about information transfer, the experienced users had a slightly higher level of concern regarding information transfer. Experienced users were also more concerned with notice / awareness and access / participation. Novice users, on the other hand, were more concerned about information storage, information collection and personalization. We attribute the experienced user concerns higher concerns with their familiarity about how the Internet works and what is or isn't possible on the Web. Novice users, in contrast, do not have such a clear understanding of the Web. They do not understand the limitations and advantages of personalization. When a website uses a cookie to remember a user's name and provide a personalized welcome message, novice users may experience uncertainty as they do not understand how such personalization is accomplished in an unobtrusive way. Since the majority of Internet users (75%) are novice Web users, website privacy practices must be conveyed to users in a way that speaks to the novice user.

	Novice	Experienced	All Users
Transfer	4.77	4.81	4.78
N/A	4.65	4.71	4.67
Storage	4.59	4.47	4.56
Access / Participation	4.35	4.40	4.36
Collection	3.97	3.73	3.91
Personalization	3.53	3.31	3.48

Table 4. Factor Means of User Concerns -- Ordered from the Total Sample's Highest Concern to Lesser Concerned

Should it really be the consumer's burden if they do not read, or understand the privacy policy? Ideally it should be the organization's responsibility. When given the option to exercise choice, consumers do not always see the benefit in doing so once they realize what choice really involves (e.g., reading a privacy policy that is extremely difficult to read, much less understand).

For years, privacy advocates have focused their ideas on notions of consumer notice and choice (e.g. having the option to opt-out or opt-in). This places the burden on the consumer and that is not fair given the high percentage of novice Web users. Numerous amounts of data exchange takes place in today's businesses; however, much of this data transfer and storage is used by honest and legitimate organizations for purposes that benefit consumers and these uses should not generate privacy concerns among consumers. What seems to concern Web consumers overall is that once their data is collected and stored, they have no control over it and it may be misused in such a way that is harmful or disruptive. Increasing transparency and stopping the practices that harm consumers is the obvious solution, but while we figure out the best approach to doing that, we suggest the following. Rather than focusing privacy protection on the presence of FIPs-based privacy policies and the ability to opt-in or opt-out, create privacy policies that consumers can understand and that address their concerns. This will, at a minimum, provide consumers with a document that pertains to their privacy protection and that is readable and relevant.

ACKNOWLEDGMENTS

The authors gratefully acknowledge Steve Scullen for his assistance with data analysis, Lynda Aiman-Smith for her assistance with survey preparation and William Stufflebeam for his assistance with survey administration. This research was supported by NSF ITR Grant #0113792.

REFERENCES

1. Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. Privacy in E-commerce: Examining user scenarios and privacy preferences. *Proceedings of the first ACM conference on Electronic commerce:*1–8.
2. Antón, A. and Earp, J. 2001. Strategies for developing policies and requirements for secure e-commerce systems," In *Recent Advances in E-Commerce Security and Privacy*, A. K. Ghosh (Ed), Kluwer Academic Publishers: 138 - 145.
3. Antón, A., Earp, J., Bolchini, D., He, Q., Jensen, C. and Stufflebeam, W. 2004. "The Lack of Clarity in Financial Privacy Policies and the Need for Standardization," Forthcoming in *IEEE Security and Privacy*.
4. Antón, A., Earp, J.,and Carter, R. September 9-10, 2002. Aligning software requirements with security and privacy policies. *Proceedings of the Eighth international Workshop on Requirements Engineering: Foundation for Software Quality.*
5. Antón, A., Earp, J. and Reese, A. 2002. "Analyzing web site privacy requirements using a privacy goal taxonomy," *10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02),* Essen, Germany, pp. 23-31, 9-13 September**.**
6. Bellotti, V. 1997. Design for privacy in multimedia computing and communications environments. In *Technology and Privacy: The New Landscape*, Philip E. Agre and Marc Rotenberg (Eds). Cambridge: MIT Press: 63-98.
7. Bentler, P. 1990. "Comparative fit indexes in structural models," *Psychological Bulletin,* vol. 107, pp.238-246.
8. Byrne, B. 1998. *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS: Basic Concepts, Applications, and Programming*, Mahwah, N.J.: L. Erlbaum.
9. Clarke, R. 1999.Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42: 60-67.
10. *The Code of Fair Information Practices*, 1973. U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, viii, http://www.epic.org/privacy/consumer/ code_fair_info.html.
11. Cranor, L., Reagle, J. and Ackerman, M. 2000. "Beyond concern: understanding net users' attitudes about online privacy," in *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*, Ingo Vogelsang and Benjamin M. Compaine (Eds.) Cambridge, MA: The MIT Press, pp. 47-70.
12. Culnan, M. 1999. "Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission," Technical Report, Georgetown University. Accessed 12/2002 at http://www.msb.edu/faculty/culnanm/GIPPS/mmrpt.PDF
13. Earp, J., Antón, A. and Aiman-Smith, L. 2003. "Crossed Signals: What Users Really Want from Internet Privacy Policies." *The Academy of Management*, August.
14. Earp, J. and Baumer, D. 2003. Innovative web use to learn about user behavior and online privacy. *Communications of the ACM*, April, pp. 81-83.
15. Federal Trade Commission, 1998. *Privacy Online: A Report to Congress*, http://www.ftc.gov/ reports/privacy3/, June.
16. Federal Trade Commission, 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, A Report to Congress.
17. Harris, Louis and Associates and Alan F. Westin. 1991, 1994, 1996, 1998. *Harris-Equifax User Privacy Surveys*. Atlanta, Ga. Equifax Inc.
18. Jones, S. Wilikens, Morris, M.P. and Masera, M. 2000. Trust requirements in e-business. *Communications of the ACM*. 43: 80-87.
19. Liu, C. and Arnett, K. 2002. "An examination of privacy policies in Fortune 500 web sites." *Mid-American Journal of Business*, Spring, 17, 1 pp.13-21.
20. Electronic Privacy Information Center, 1999. Surfer Beware III: Privacy Policies without Privacy Protection, http:www.epic.org/reports/surfer-beware3.html, , December.
21. Mason, R. 1986. Four ethical issues of the information age. *MISQ,* 10: 4-12.
22. Nunnally, J. 1978. *Psychometric Theory,* New York: McGraw Hill.
23. Organisation for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 1980. Last accessed on May 12, 2003 at http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html.
24. National Telecommunications and Information Administration. 2002. A Nation Online: How Americans Are Expanding Their Use of the Internet http://www.ntia.doc.gov/ntiahome/dn/ Washington, D.C. February.
25. Kasanoff, B. 2001. *Making it personal*. Cambridge, MA: Perseus Publishing.
26. Ranganathan, C. and Ganapathy, S. 2002**.** Key dimensions of business-to-user web sites. *Information and Management*, 39: 457-465.
27. Raul, A P. 2002. *Privacy and the digital state: Balancing public information and personal privacy*. Boston, MA: Kluwer.
28. Roth, P., Switzer, F. and Switzer, D. 2002. "Missing data in multiple item scales: a monte carlo analysis of missing data techniques," *Organizational Research Methods*, vol. 2, pp.211-232.
29. Rust, R., Kannan, P.; and Peng, N. 2002. The customer economics of internet privacy. *Journal of the Academy of Marketing Science*, 30:455 – 464.