

# Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality of Compliance

**Kathy Stewart Schwaig**  
Kennesaw State University

**Gerald C. Kane**  
Emory University

**Veda C. Storey**  
Georgia State University

## **Abstract**

*Corporate information privacy policies are receiving increased attention in the information privacy debate. Prior studies used Web surveys to analyze the content of online information privacy policies and to assess whether or not the policies comply with a standard known as the Fair Information Practices. One assumption of these studies is that the main role of a privacy policy is to protect the consumer by communicating a firm's information practices. This paper employs Habermas's Theory of Communicative Action to uncover the much more complex and multifaceted roles that privacy policies actually play in a social context. Overall, the study's findings offer insights into the reflective nature of information privacy policies, specifically their role in social interactions among companies, consumers and government regulators. The theoretical and managerial implications of the results are discussed and directions for future research provided.*

**ACM categories:** K.4, K.4.2, K.4.3, K.4.4

**Keywords:** information privacy, Web surveys, Internet, electronic commerce

## **Introduction**

Consumers' concerns about information privacy are at the forefront of policy and ethical issues associated with the information age, especially in the United States (Caudill & Murphy, 2000; Smith, et al., 1996). The lack of consumer confidence in online privacy is the most often cited reason for not shopping online (Turner & Dasgupta, 2003; Hoffman et al., 1999; Porter, 2000). Firms use consumer data to personalize products and services and to amass profiles of individuals (Liu & Arnett, 2002; Stewart & Segars, 2002). Some consumers and privacy advocates, however, are concerned that companies will violate an individual's privacy and use their personal information without informed consent (U.S. Public Interest Research group 2000; Hann et al., 2002).

The issue is of interest to policymakers with respect to both protecting consumers' privacy rights and facilitating the continued growth of e-commerce and the resulting benefits for both business and consumers (Miyazaki & Fernandez, 2000). Smith (1993) called for a *workable societal objective* where the rights of consumers are balanced against the desires of corporations and the needs of society for consumer personal information. The Federal Trade Commission has recommended that the U.S.

♦ <b>Notice/Awareness:</b> consumers should have notice of an organization's online information practices
♦ <b>Choice/Consent:</b> consumers should have a choice about the use and dissemination of information they reveal, usually through an opt-in or opt-out mechanism
♦ <b>Access/Participation:</b> consumers should have access to the information businesses collect about them to help ensure accuracy and completeness
♦ <b>Integrity/Security:</b> consumers should have the personal information collected about them adequately secured from outside parties and from corruption of the data
♦ <b>Enforcement/Redress:</b> consumers should have a way to ensure that businesses and organizations comply with these core privacy principles either through external regulation (audits) or certification programs

**Table 1. Fair Information Practices**

Congress increase information privacy legislation directed at Internet firms. However, the model to date in the United States continues to be self-regulation<sup>1</sup> even though many consumers and privacy advocates believe that federal and state governments should pass laws regulating how personal information is collected and used on the Internet (Garfinkel, 2002; Liu & Arnett, 2002).

One objective of self-regulation is for firms to implement Fair Information Practices that guide their collection, use and sharing of consumer personal information gathered online (Milne & Culnan, 2002). Understanding the degree to which self-regulation works is an important policy issue in the debate (Milne & Culnan, 2002). One method of assessing the effectiveness of self-regulation is to study the stated information practices of firms (Culnan, 2000; Milne & Culnan, 2002; Liu & Arnett, 2002).

Web surveys of online information privacy policies have become increasingly popular with the growth of e-commerce (Culnan, 2000; Milne & Culnan, 2002; Federal Trade Commission, 2000; Liu & Arnett, 2002). Web surveys focus mainly on two questions: 1) to what extent are firms posting information privacy policies online, and 2) to what degree do these policies conform to a set of standards known as the

<sup>1</sup> Self-regulation requires that industries develop rules and regulations, as well as enforcement mechanisms, that replace government regulation (Swire, 1997). At a minimum, firms develop information practices based upon acceptable standards and communicate these practices via privacy policies to the consumer. Self-regulation is the model most frequently applied in the United States and the remainder of the paper is based upon this perspective.

Fair Information Practice (FIP)? Fair Information Practices are defined as representing the “global principles that fairly balance the need for business to collect and use personal information with the legitimate privacy interest of consumers to be able to exercise control over the disclosure and subsequent uses of their personal information.” (Milne & Culnan, 2002, p.3). The Fair Information Practices are summarized in Table 1.

Self-regulation is deemed to be working if more firms are posting policies and more firms are complying with FIP over time. Implicit in this line of thinking is the notion that privacy policies are a surrogate for consumer protection. In other words, *privacy policies exist primarily as a mechanism to protect the consumer.* For example, Liu and Arnett (2002) state:

“In order to ease customers’ concerns about online privacy, public Web sites have begun to post privacy policies or statements regarding online collection, use, and dissemination of personal information.” (p.14)

Milne and Culnan (2002) argue that:

“Privacy notices should serve as a source of information to help consumers to make better choices about the risk versus benefits of disclosing their personal information and should help people make choices in some of the same ways that product labels help inform choices among competing products including avoiding products that present some type of health or other risk.” (p.357)

In light of the consumer protection orientation of past Web surveys, the findings have been somewhat disappointing. Although the quality of policies has steadily improved over time, most web surveys suggest that privacy policies are inadequate and fail to effectively protect the privacy rights of consumers (Milne & Culnan, 2002).

Indications are that the consumer protection perspective towards online privacy policies is too limited, and in fact, may bias the researchers’ interpretation of their studies’ findings. Recent studies have indicated that online consumers rarely even read privacy policies and, when they do, find them to be too long and full of confusing legal jargon (Culnan & Milne, 2001). Two questions then arise.

The first relates to the reasons firms invest organizational resources in a consumer protection mechanism that consumers rarely access; the second, the reasons why researchers rely on compliance to FIP as a measure of whether or not self-regulation is working and as a surrogate for consumers protection.

The objective of this research is examine these two questions and, in doing so, develop a theoretical framework to assess the real role of information privacy policies in organizations. The Theory of Communicative Action (Habermas, 1978; Habermas, 1984; Habermas, 1987), is used to identify the true purpose of privacy policies and the roles they play within organizations. The contribution of this research is to challenge the traditional assumption that privacy policies are primarily a communication mechanism for the benefit of consumers. The research shows that, despite their widespread use, privacy policies may actually enable firms to act in their own self-interest and at the expense of the consumer. Although privacy policies may reflect a number of distinct social interactions among companies, consumers, and government regulators, results indicate that their primary role is one of *strategic action* whereby companies use privacy policies to create a trustworthy image in the marketplace.

The remainder of the paper is organized as follows. The next section, Theoretical Development, reviews Critical Social Theory and Habermas' Theory of Communicative Action. An outline of the methodology used in this study is then presented. The Analysis section interprets the data in light of Habermas' theory. Concluding remarks and implications for future research are provided in the Conclusion.

## Theoretical Development

### Critical Social Theory

Critical Social Theory has been discussed extensively in information systems, general management and social sciences research (Schultze & Leidner, 2002, Ngwenyama & Lee, 1997). Traditional social scientists view their work as complete when, after observing some phenomenon, it can be explained and understood. Conversely, critical social theorists believe that inquiry into social activities should not be isolated from the social context and the world of the real participants. One goal of critical research is to untangle the multiple and disconnected meanings inherent in a given context and to provide a clearer picture of the underlying social structure (Schultze &

Leidner, 2002).<sup>2</sup> By analyzing and challenging the nature and purpose of social actions, the critical researcher seeks to emancipate those manipulated by the social structure and to initiate a dialogue geared towards restoring equitable relationships among parties (Schultze & Leidner, 2002).

In the case of online privacy policies, a number of distinct actors are involved: namely, government legislators, corporations and consumers. The political and social interactions among these actors are partially embodied in the text of online privacy policies. Previous research that attributes privacy policies as representing only one meaning—communicating privacy practices as a consumer protection mechanism—fails to account for the multivalent structure embedded in privacy disclosures.

### Habermas' Theory of Communicative Action

This study uses the critical social theory of Habermas (1979, 1984, 1987). Applied extensively as a basis for critical research in information systems (Hirschheim & Klein, 1994; Lyytinen, 1992; Lyytinen and Klein, 1985; Mingers, 1981; Ngwenyama 1987; Ngwenyama 1991; Ngwenyama & Lee, 1997; Lyytinen & Hersheim, 1988), Habermas' theory of social communication suggests that a certain set of norms underlie all social action or intentional behavior conducted in good faith, and that both individuals and organizations accede to these norms when engaging in social communication. Habermas' theory identifies four ideal types of social action: communicative, instrumental, discursive and strategic. Each social action has a specific focus, but, taken together, the four represent various aspects of human behavior in social contexts. (Ngwenyama & Lee, 1997). Each action type is defined below:

1. *Communicative action* -- the actors involved in communicative action are equal, seeking to create a mutual understanding of behavior. Communicative action is based on the 'consensual norms' which define behavioral expectations within a communication context (Lyytinen & Hersheim, 1998).
2. *Instrumental action* -- one actor treats the other as it would an object or subservient without free will; for example, a military officer giving an order to a lower-ranking officer. Little social negotiation takes place since enlisted personnel are expected to carry out the orders of an officer without hesitation.

---

<sup>2</sup> Here the lines blur somewhat between what Schultze and Leidner (2002) identify as the critical and dialogic discourses. This perspective is consistent with previous critical research (Ngwenyama & Lee, 1997), as well as Schultze and Leidner's own recognition of the relatedness of these two paradigms (p. 217).

3. *Discursive action* – actors negotiate when social norms are in doubt or when one actor seeks to restore the relationship with another by proving the validity of the actor’s intention and the actor’s desire to establish a strong relationship.

4. *Strategic action* -- actors treat other actors as intelligent agents, seeking to convince the other of a particular point-of-view or move the other to a particular action. An agent will engage in strategic action in an attempt to persuade or manipulate the other party into a particular desired social action.

Critical social theory recognizes that any social action between two parties might not conform to its related expected norms (Ngwenyama & Lee, 1997). Each of the four social actions, therefore, carries with it a set of validity claims that can be used to test distorted communication. The test results allow the listener or reader to determine if the communication was false, incomplete, insincere, or unwarranted (Ngwenyama & Lee, 1997) A particular communicative action is tested against its relevant set of validity claims to determine whether it is an appropriate and effective expression of the communicative purpose. When social action does not adhere to its validity claims, the other actors involved in dialogue will then seek either to engage in dialogue to restore the communicative norms or to sanction the violator. The set of validity claims related to the four social actions are described below. Table 2 identifies which validity claims are appropriate for a given social action (Habermas, 1979).

- *Contextuality / appropriateness* -- the degree to which the action fits the social norms and expectations for a social action.
- *Completeness* -- the degree to which an action includes or omits components that are necessary for understanding or enacting a social action.
- *Truthfulness* -- the degree to which communicative actions are valid when compared to experience or other evidence.
- *Sincerity* -- the depth of the sincerity of the claims, reflecting whether an actor is truly motivated to conduct a social action.
- *Clarity / comprehensibility* -- the degree to which the intended content of the communicative action is easily and effectively understood, including the use of jargon or the use of proprietary words and phrases to engage in the action.

For privacy policies, one would expect that communicative action is the most common paradigm given that privacy statements exist, presumably, to create a mutual understanding of appropriate corporate behavior. As mentioned earlier, past Web

Social Action	Validity Claim
Communicative	Contextuality, Completeness, Truthfulness, Clarity,
Instrumental Discursive	Contextuality, Truthfulness, Sincerity, Clarity, Contextuality
Strategic	Sincerity, Contextuality

**Table 2. Communicative Actions and Validity Claims**

surveys assumed the communicative role and viewed privacy statements as consumer protection mechanisms that enable consumers to make educated decisions about whether or not they should disclose their personal information to the firm.

The following section discusses the data gathering process, and then the data are analyzed in light of the validity claims associated with the view of privacy policies as communicative action. Other types of social action are then examined to assess whether multiple social actions are indeed embedded within the text of privacy policies.

## Methodology

A content analysis of the online privacy policies of the Fortune 500 was conducted. The Fortune 500 firms are recognized as leaders in their respective industries and in the use of information technology (Liu & Arnett, 2002; Li et al., 1993; Li et al, 2001; McLeod & Rogers, 1982). With the maturing and incorporation of e-commerce practices by both business to consumers (B2C) and business to business (B2B) firms,<sup>3</sup> privacy issues for large firms are of increasing importance as consumers engage in e-commerce activities that collect personal information (Liu & Arnett, 2002).

Modeled after the 1999 Georgetown Study (Culnan, 2000) and the 2000 Federal Trade Commission Study (Federal Trade Commission, 2000), the current research uses a modified version of the previous instruments. The researchers used links from the *Fortune* Web site to access each firm’s site. The site was examined for a privacy policy. If a policy was found, the survey was completed; if not, only the first 5 demographic-type questions were answered. One researcher collected the data from all 500 sites. Two other researchers independently reviewed a random sample of the 500 sites with a resultant inter-rater

<sup>3</sup> Although the information privacy debate often focuses on B2C firms, the study found that B2B firms also post information policies and collect personal information.

reliability of 89.23%. An electronic copy of each privacy policy was made in case subsequent changes or updates to the policy occurred. Software-assisted keyword analysis was conducted, as was a qualitative assessment of the language and style of the policies.

## Analysis

**Privacy Policies as Communicative Action.** As noted above, the most common interpretation of online privacy policies is communicative action. Communicative action seeks to convey information regarding consensual norms or behavioral expectations, between equal partners. In the case of online privacy policies, a company expresses the norms for collecting and handling consumer information through communicative action. Theoretically, consumers benefit from the communicative role of online disclosures because they can use the information in the policy to make an informed decision as to whether or not to provide the site with personal information.

Past studies assume the communicative role using privacy policies as a proxy for actual privacy practices (Milne & Culnan, 2002). If the primary purpose of privacy policies is to communicate privacy practices, then the four validity claims of communicative action should be met. To test this assumption, the validity claims 1) contextuality, 2) completeness, 3) clarity and 4) truthfulness are applied to the privacy policies to assess whether online disclosures meet the standards set forth by Habermas (1979, 1984, 1987).

**Communicative Action Validity Claim: Contextuality.** The contextuality claim suggests that all communicative action is embedded in organizational context and this context defines appropriate and reasonable behavior (Ngwenyama & Lee, 1997). In the case of online policies, this context serves as a frame of reference that enables consumers to interpret the meaning and actions of firms. To meet contextuality claims, a privacy policy should include statements and afford protections that are reasonable and sensible given the context of the relationship between the firm and the consumer.

In order to analyze the contextuality claim, each site was classified as either a high information collector or a low information collector. That is, some Web sites are intentionally designed to collect information from consumers for purposes of interaction, whereas other sites are designed for one-way information flow, intended only to provide information to the customer. The validity claim of context would suggest that high information collectors should have more detailed and more prominently displayed privacy policies than would low information collectors. Our analysis

suggests that this is not the case. A small number of sites actually collect no information but still have privacy policies. Even though the context offers no reason for the provision of a privacy policy, these companies do so anyway. Furthermore, other low information collectors do collect some information, but in a relatively obscure section of the site, such as the "careers" section. One might expect that context would dictate a somewhat lower prominence of privacy policies on these sites as well, but most low information collectors display and craft privacy policies in much the same way as high information collectors. Thus, companies are clearly outlining detailed privacy policies, even in contexts where extensive protection is neither clearly offered nor necessary.

A second contextuality validity claim tested was with respect to children. The Children's Online Privacy Protection Act of 1998 (COPPA) requires sites that collect information from children to explicitly state so in their policies and to gain parental consent before collecting information from children. Forty percent of the sites with policies mention children to some extent. Of these, 65% define children as being under 13 years of age consistent with COPPA. Ironically, the group of companies that had special protections for children did not come from the expected context. For example, the privacy policy of one of the largest petrochemical companies<sup>4</sup> in the world claims:

The Site contains information that may be of special interest to children, but Alpha Company does not seek through the Site to gather Personal Information from or about persons under the age of 17.

Similarly, the privacy policy of a large telecommunications company contains the following, rather long and tedious section:

Beta Company joins the industry in recognizing that children, including young teens, may not be able to make informed choices about personal information requested online. Accordingly, Beta Company does not target children or teenagers (younger than eighteen years of age) for collection of information online. Beta Company does not solicit or collect customer identifiable

---

<sup>4</sup> Although the information gathered is publicly available, we have chosen not to specifically name the organizations from whose web sites we quote. Our intent is not to single out particular organizations, but to provide examples that were representative of the sites we studied.

information targeted at children and teenagers under eighteen and does not allow anyone else to do so on a Beta Company Web site. In addition, the editorial content of Beta Company Web sites designed for children will not knowingly promote or link to any third party Web site that collects customer identifiable information unless that Web site publishes a privacy policy that is easily accessible. In addition, on all of its online services and Beta Company Web sites, Beta Company will encourage children to seek the consent of their parents before providing any information about themselves or their households to anyone on the Internet. Beta Company encourages parents to take an active role to protect the privacy and security of their children and to prevent the inappropriate use of information about their children. Beta Company supports the development of technologies that help parents to control the collection and use of personal information from children who use online services in their households.

This statement comprises approximately 20% of the total content of the privacy policy, even though neither the site nor the company is appreciably geared to children. Furthermore, office supply retailers, agricultural manufacturers, insurance companies, tire companies, business service companies have significantly more robust statements about children than do many toy stores, soft drink manufacturers, and fast-food restaurants. If the privacy policies met the contextuality claim for communication, a clearer association would exist between policies that offer special protection to children and companies geared towards children.

Third, the contextuality validity claim does not support the communicative action role in relation to the recourse offered to consumers if they do not agree with the practices outlined in the privacy policy. In this case, the most frequent recourse offered is "don't use the site." Consider, for example, the following statement:

"If you are dissatisfied with any portion of the Site or the Services or with any of these terms, your sole and exclusive remedy is to discontinue using the Site and the Services."

In the case of third-party cookies and other data collection practices, it would be too late for a consumer to simply discontinue use of the site by the time they read the policy. By simply viewing the privacy policy, personal information may have been surreptitiously collected subjecting the individual to the privacy practices of the site. The context of online privacy dictates that, if privacy protection is the primary function of policies, then customers should have the right to examine a privacy policy *before* being subject to the consequences of the firm's information practices.

**Communicative Action Validity Claim: Completeness.** The validity claim of completeness suggests that a company will comprehensively address the privacy concerns of consumers. Completeness is analyzed along three measures: 1) its adherence to the FIP standard, 2) scope of the policy, and 3) longevity of the policy.

*Adherence to FIP:* The most fundamental understanding of completeness is in relation to adherence to the FIP. The FIP has been accepted as the general template for addressing privacy concerns. If firms are concerned with offering complete policies, they will likely address each FIP component. Analysis of the degree of compliance (completeness) to the FIP among the *Fortune* 500 shows that most privacy policies are not complete. Table 2 presents the results. Of the 383 Web sites that collect personal identifying information and post a privacy policy:

- 98% include at least one survey item for notice;
- 62% include at least one survey item for choice;
- 45% include at least one survey item for access;
- 70% include at least one survey item for security.

Only 31% of policies contain one or more survey items for all four elements of Fair Information Practices. The policies are also examined to determine if any include all measured items of the four elements of the Fair Information Practices. Of the 383 Web sites that collect personal identifying information and post a privacy policy, only 3% of the policies contain all survey items for all four elements of Fair Information Practices. In summary, an extremely low percentage adhere to all categories of the FIP completely (3%) or even in part (31%).

2. *Scope of policy:* A second dimension of completeness concerns the scope of protection offered by the policy. That is, how completely does the privacy policy protect the online experience of the consumer? Scope is defined in two ways: 1) Are the

Policies	Frequency	Percentage (Base =383)
Mentions at least one item for Notice	376	98
Mentions at least one item for Choice	236	62
Mentions at least one item for Access	172	45
Mentions at least one item for Security	268	70
Mentions at least one item each for Notice, Choice, Access & Security	119	31
All of Notice <sup>5</sup>	336	88
Choice Combined <sup>6</sup>	111	29
Access <sup>7</sup>	69	18
Security <sup>8</sup>	190	50
Mentions Notice, Choice, Access & Security <sup>9</sup>	14	3

**Table 3. Policies that Included Elements of Fair Information Practices**

protections in the policy applicable to the whole site, and 2) are the protections in the policy applicable to the firm only or also to its business partners, affiliates, subsidiaries, etc.?

Forty-five (45%) percent of the policies fail to mention anything about the applicability of the site. In some cases, the policy is explicitly not applicable to the entire site; rather, the consumer must check for amendments to the privacy policy on a page-by-page basis. For example,

You are advised to check each page you visit on the Site. Some locations may have special additional terms and conditions that apply to use of or interaction with that location. These terms and conditions may also be changed at any time without notice. Your use of that location constitutes your acceptance of those special additional terms and conditions.

Furthermore, many of the sites that limit applicability of the privacy policy to the site alone, reserve the right to freely share information with others, giving no indication of what standards will be applied to the handling of personal information once it reaches the hands of the partners. One policy included the following:

Your privacy is important to us. We would never share your personal information with a third party. We will, however, from time to time, provide your personal information to our business partners and affiliates so that they might contact you with offers in which they think you might be interested.

As illustrated in the example, firms use terms like “business partners” and “affiliates.” In most cases, the policy does not name the firm. In fact, only 2% of the policies explicitly state that the policy is applicable to all business partners and affiliates. Consumers are left to assume that business partners and affiliates are held to the same standards as the firm, even though this is not stated in the policy.

**3. Longevity:** Firms are expected to update their policies over time. Policies that warn consumers about pending changes and their implications to personal information already collected as well as data that may be collected in the future are deemed to be more complete. The vast majority of sites report that they reserve the right to change the privacy policy at any time and without notice. Only 54% of the sites with policies mention a process should changes occur; of these, only 2% provide a time frame within which to expect a change. For example, one policy stated:

We reserve the right to change, modify or amend this policy at any time. Please check our Privacy Policy periodically for changes. Use of this Gamma Company web site after modification implies that you consent to this Privacy Policy as modified.

<sup>5</sup> Sites that had a privacy policy and mention **all** items for Notice.  
<sup>6</sup> Sites that mention **all** items for Choice.  
<sup>7</sup> Sites that mention **all** items for Access.  
<sup>8</sup> Sites that mention **all** items of Security  
<sup>9</sup> Represents the number of sites that mention **all** items for Notice, Choice, Access and Security.

No information is provided on what happens to existing information once the privacy policy changes. Furthermore, these changes are immediate and it is the customer's responsibility to monitor them. Thus, whether defined in terms of adherence to the Fair Information Practices, the scope of the policy or the longevity of the policy, privacy policies in general do not uphold the validity claim of completeness.

**Communicative Action Validity Claim: Clarity.**

The validity claim of clarity suggests that, if communication is the primary function of a policy, then it should be written in language easily understood by the consumer. Prior studies analyzed the "readability" of privacy disclosures, finding that the average grade-level required to understand a policy is between 11.5 and 14.5 (Milne & Culnan 2002).

English is the first language of the research team conducting the study. In addition, the team is well versed in the privacy issue and related vocabulary and terminology. Nonetheless, the team had difficulty identifying what kind of protection is offered by many of the policies, and in some cases, had to read passages three and four times to ascertain the meaning.

In addition to readability, the style appears more to conceal the protection offered by policies than to clarify. Many policies follow a common stylistic pattern of making a bold sweeping claim of privacy protection and then qualifying the protection in subsequent statements. For example:

We do not sell your personal information to anyone. The law allows you to "opt out" of only certain kinds of information sharing with third parties. Zeta Company does not share personal information about you with any third parties that triggers this opt out right. This means YOU ARE ALREADY OPTED OUT [emphasis in original]. Zeta Company only shares personal information with third parties in the following limited circumstances:

- We disclose personal information to companies that help process transactions
- Sometimes we enter into contracts with third parties so that they can assist us in servicing your account
- We may also enter into what is called a "joint marketing

relationship" with another financial institution, if we believe that you might be interested in hearing about its products or services

- We may disclose or report personal information in limited circumstances where we believe in good faith that disclosure is required or permitted under law

The implication in this policy is that the consumer is only harmed if Zeta Company "sells" personal information. In the list of exceptions, Zeta Company reserves the right to partner with other firms in direct marketing products to the consumer, based upon the information provided. Although the statement implies that a consumer may choose to opt-out of receiving offers, a careful reading of the statement reveals that the consumer *does not* have the option to opt-out. Thus, this common stylistic pattern is geared more towards hindering clear communication rather than enhancing it.

A final means of assessing the clarity of the policy is the relative accessibility of a policy to the consumer. If the primary purpose of a privacy policy is to communicate practices to consumers, it would follow that policies should be clearly and explicitly posted on a Web site. Surprisingly, ten percent (10%) of the firms that collect personally identifying information do not post a privacy policy. Fifteen percent (15%) of the firms that have a policy fail to provide a link to the policy from the site's home page. For one prominent retail company, the researchers had to perform a keyword search on the word "privacy" to locate the privacy policy. Considering their readability, style, and location within the website, privacy policies seem to fail to adhere to the validity claim of clarity.

**Communicative Action Validity Claim: Truthfulness.**

The validity claim of truthfulness suggests that the policy should be comprised of believable statements that accurately communicate the information practices of the firm. The policies violate the truthfulness claims in both explicit and implicit ways. As mentioned earlier, many sites contain bold claims about not collecting information from children. Several of these sites, however, fail to include any form of age verification. In these cases, it is unclear how a policy of not collecting information from minors would actually be recognized or enforced.

The study uses "participation in a privacy program" (Benassi, 1999) as a proxy for truthfulness. These programs (Better Business Bureau Online and Trust-e) require that a firm's information practices be

Validity Claim	Result
Contextuality	<i>Some support</i>
Completeness	<i>Little support</i>
Clarity	<i>Little support</i>
Truthfulness	<i>No support</i>

**Table 4. Results of validity claims for communicative action**

independently audited by an outside firm. If the information practices are found to be consistent with their stated information policy, the firm passes the audit and is allowed to display the seal on its Web site. In other words, the firm's information policy *truthfully* represents the information practices of the firm. Only 7% of the firms that collect personally identifying information participate in privacy seal enforcement programs. Such low participation suggests that validating the truthfulness of privacy policies is not a high priority for firms, weakening the validity claim of truthfulness.

In sum, the validity claims of online privacy policies as communicative action are not strongly supported as shown in Table 4. There are two possible interpretations for these results. First, privacy policies may, in fact, serve a communicative role. If so, the results of this study complement those of past web surveys that found that privacy policies may prove even more inadequate than previously thought. Although companies may fare well on a cursory comparison to the FIP, a more detailed examination reveals that the completeness, truthfulness, clarity and context of these policies are questionable. Second, privacy policies may actually serve functions other than communicating information practices. This explanation is investigated in the next section where Habermas's framework is applied to uncover other social actions enacted through privacy policies.

**Other social functions of privacy policies.** The first step in understanding other social actions is to recognize that multiple actors—companies, consumers and governmental regulators—are involved in the social interaction. Presumably, each group has a certain measure of control over the other. Consumers can exercise purchasing and investing power over companies and provide tax dollars to and exercise voting control over the government. Governments regulate both companies and individuals, and are expected to oversee those relationships in a way that is equitable for all involved. Companies provide tax dollars for governments and jobs and products for consumers. In some cases, such as the sale and purchase of physical goods, the laws and norms governing the behaviors among the actors are well established. In other cases, such as

online privacy, these relationships are still under negotiation.

Thus, privacy policies are understood as representing various facets of this developing relationship among companies, customers and governments in the social world of online interaction. In addition to the limited role of communicative action already addressed, privacy policies encompass the other social actions discussed by Habermas—instrumental, discursive and strategic action. Some support exists for each of the social actions, consistent with the notion that the categories are ideal types and any actual communication may contain elements of more than one. Nevertheless, one category is likely to be dominant in a given situation. Each remaining social action is analyzed in the context of the *Fortune* 500 and discussed below.

### Privacy Policies as Instrumental Action

Another role that online policies may play in the social interaction among the players in the information privacy debate is one of instrumental action. Understood as one social actor issuing a command to another, instrumental action is viewed as *purposive action* where the communicating actor attempts to achieve measurable objectives often at the expense of the other actor. Instrumental action is directed towards agents as if they were inanimate objects that can be manipulated to serve the actor's needs (Lyytinen & Hirschheim, 1988). The second actor has a socially compelling reason to obey the order without question.

In the context of information privacy policies, instrumental action is seen when firms communicate their information practices to consumers for their own self-serving purposes and often at the consumer's expense. For many firms, information privacy policies are primarily a mechanism for either enabling continued self-regulation or are a response to existing government regulation.<sup>10</sup> As government agencies or industry regulatory boards issue mandates, information privacy disclosures are one way firms respond and seek compliance. After posting a privacy policy, a firm is bound by legal obligations to adhere to the privacy protections and practices it offers. Firms, therefore, may try to limit their liability or make it difficult for the consumer to understand just

<sup>10</sup> For example, the Gramm-Leach-Bliley Act requires financial institutions to disclose their information practices to consumers on an annual basis; likewise, the Health Insurance Portability and Accountability Act of 1996 requires healthcare professionals to disclose their information practices and restricts the sharing of personal medical information in some instances without the patient's consent.

what protections are afforded. In their instrumental role, privacy policies are written more to limit potential legal threats or thwart possible government intervention than they are to protect the consumer.

#### **Instrumental Action Validity Claim: Contextuality.**

The only validity claim applied to instrumental action is context, whether or not one actor has the authority to issue mandates to another. Corporations clearly have a responsibility and sometimes legal obligation to communicate their information policies to consumers. Clearly, firms view their information privacy policies as an obligatory response to government mandates. For example, when conducting background research for this study, the researchers contacted a technical writer who was responsible for authoring a *Fortune* 500 privacy policy. She commented:

“It is very important that we write these policies in a way that we will not be caught violating them. It’s better not to have a privacy policy at all than to violate the one you have established....that can get you into real trouble.”

Furthermore, the language of many of the policies in the study indicates that firms are more concerned about protecting themselves legally than they are about protecting the consumer. The ambiguous and obtuse statements afforded consumers do little more than decipher. create confusion in the way “protections” are presented. Some sites have legal notices separate from their privacy policy to address issues such as copyright protection and contractual obligations. In many cases, however, sites explicitly intermingle their legal disclaimers and their privacy policies. For instance, after clicking the link for “privacy” on the Website of a major hotel chain, the statement begins:

Important! This is a binding legal agreement (this "agreement"). Please read these terms and conditions of use carefully before using this site. This Agreement governs your use of this site (collectively, the "Site") and is by and between Nu Corporation (referred to herein as "NC", "we", "us", or "our") and you, on behalf of yourself and the buyer, member or supplier for which you have registered ("you"). By using, viewing, transmitting, caching, storing and/or otherwise utilizing the Site, the services or functions offered in or by

the Site and/or the contents of the Site in any way, you have agreed to each and all of the terms and conditions set forth below, and waive any right to claim ambiguity or error in this Agreement.

Other evidence of firms being more concerned about legal issues rather than privacy concerns was presented earlier in this study. Examples include firms limiting the applicability of the policy to only themselves while sharing personal information with third parties, as well as firms limiting the scope of the privacy policy to only a portion of the site. Restricted scope clearly limits the liability of the firm and weakens whatever protection the policy offers. Finally, sites also limit their liability by reserving the right to change their policy without prior notice. It is clearly more difficult to hold a company accountable for its information practices when the firm can alter their policy at any time. Therefore, evidence exists for privacy policies as mechanisms of instrumental action in that they may fulfill a self-serving need of the firm at the expense of real consumer protection.

#### **Privacy Policies as Discursive Action**

Another possible role that online privacy policies play in the social interaction among companies, consumers, and governmental regulators is discursive social action. Actors engage in discursive action when seeking to develop or restore trust in a tenuous social relationship. Online privacy has been a significant issue since the earliest days of e-commerce. Some firms received negative publicity and experienced consumer backlash when it was discovered that they were using technologies such as cookies and other data-collection mechanisms. One function of privacy policies, therefore, is to restore the relationship with online customers in the wake of evolving privacy concerns. The fair information practices represent the *terms of agreement* in the debate.

Two validity claims are associated with discursive action: 1) truthfulness, and 2) clarity. Although each was analyzed earlier in terms of communicative action, each plays a slightly different role with regard to discursive action. In the communicative action context, truthfulness and clarity were judged in relation to the privacy practices themselves. With discursive action, truthfulness and clarity are understood in the context of facilitating and restoring the relationship between relevant actors. Thus, it is possible for truthfulness and clarity to be challenged in their communicative role but remain valid in their discursive role.

**Discursive Action Validity Claims: Truthfulness.** Since the fair information practices are the terms of agreement, evidence exists that companies are seeking to improve and restore the relationship with relevant parties. Since evaluation of online privacy policies began in 1998, both the degree of compliance with the Fair Information Practices and the number of firms posting policies has increased (Milne & Culnan, 2002). The results of the current study support this finding. Therefore, when companies claim that they are interested in protecting consumer privacy, some evidence exists to support the truthfulness of that claim.

**Discursive Action Validity Claims: Clarity.** If companies want to restore their relationship with consumers and if FIP is the standard by which to do so, they are expected to adhere explicitly and unambiguously to the Fair Information Practices. Despite earlier evidence of companies complicating their privacy policies, others read like a checklist of the Fair Information Practices. For example, the introduction of one privacy policy states:

We have established the following principles that govern our information practices:

- If we collect information from or about you, we will tell you what information is being collected, how, by whom, and for what purposes.
- We will give you options about how the personal information that you provide us may be used.
- We use recognized industry safeguards to protect customer personal information from unauthorized access or use.
- You will have the opportunity to update your personal information that you have provided to us. We will also take steps to make sure that any updates that are provided are processed in a timely and complete manner.
- We will tell you how you can contact us regarding our privacy statement and practices.

These bullets clearly outline the five elements of the Fair Information Practices—notice, choice, security, access and enforcement/redress. With one exception, these elements are even listed in the same order as contained in the Fair Information Practices. Although the specific protections granted on each point may be difficult to ascertain, the fact that these policies follow

a prescribed pattern in systematically addressing the points of the Fair Information Practices demonstrates that companies do seek to restore their relationship with consumers.

Again, note that these validity claims are related to the explicit terms of the relationship between parties, not to the privacy practices themselves. Here, discursive action should be understood as explicitly adhering to the “letter of the law” as embodied in the Fair Information Practices. Under this interpretation, evidence exists that companies are increasingly adhering to the explicit elements of the Fair Information Practices. On the other hand, adherence to the letter of the law does not necessarily imply upholding its spirit by actually extending increasing privacy protection to the consumer. In fact, the next section demonstrates some ways in which privacy policies actually serve to limit protection, all the while cultivating the image of protection.

### **Privacy Policies as Strategic Action**

The final interpretation of the social role of privacy policies is strategic action. In strategic action, one actor seeks to manipulate the other to a desired action or to create a desired impression. Many firms want to be perceived in the marketplace as being socially responsible. Information privacy is currently one of the most sensitive social issues. Firms with a proactive stance on the information privacy issue may market their position as a distinctive competence. Information privacy policies, therefore, provide firms with an opportunity to convey a socially responsible image to consumers. In response, companies hope to gain the trust of consumers so that they will provide personal information, as well as buy products and services.

In the strategic action context, it is the *image* of privacy protection that is paramount, rather than the actual *provision* of that protection. Within privacy policies, firms can cultivate the public image of privacy protector, without limiting the competitive and economic advantages leveraged through the collection and use of consumer personal information.

One of the major findings of this study is that the dominant function of privacy policies is strategic action. The role of privacy policies to support effective public relations outweighs its communicative, instrumental and discursive roles. Although each of the forms of social action is present to an extent, the use of the privacy policy to cultivate a positive image about the company is consistent across the sample.

The two validity claims for strategic action, sincerity and context are discussed below.

**Strategic Action Validity Claims: Sincerity.**

Evidence supports the notion that companies seek to express their sincere concern for consumer privacy through their privacy policies. First, the vast majority of privacy policies (80%) begin with some sort of commitment to the customer and to the protection of their privacy, often explicitly linking it to their business practices. Consider the opening statements from three policies of three different firms:

- When it comes to your financial affairs, you expect a relationship built on privacy and integrity. You can trust Omega Company to meet and exceed these expectations.
- Privacy has always been an important part of how we do business.
- For over 200 years, we've respected and protected customer privacy.

Clearly, these companies use their privacy policies to communicate a strategic message to the customer: that each firm is trustworthy and one with whom the customer can do business with confidence. Yet, these statements have no bearing on whether privacy protection is actually offered by the company. For instance, consider the following statement from one of the world's largest and most recognizable firms. It begins with a similar assertion:

You don't want your personal information to fall into the wrong hands. Neither does Epsilon Company.

Despite this bold commitment to consumer privacy, the privacy statement that follows reserves the company's right:

- to use cookies,
- to place 3<sup>rd</sup> party cookies in order to optimize advertising efforts,
- to collect and store personally identifiable information for marketing purposes, and
- to share that information with other companies.

Aside from reserving these explicit rights for the company, this particular privacy policy actually offers *no privacy protection* whatsoever for the consumer. Ironically, the statement closes with the following assertion:

You take online privacy seriously, and so does Epsilon Company. It's our way of sustaining your trust in Epsilon Company and our products and services.

This statement provides the clearest example of strategic action in which the policy seeks to convey

the public image of trustworthiness, without actually providing protection to the consumer.

Strategic action also accounts for some of the inconsistencies found in the communicative action validity claim of *context* discussed earlier. Whether or not firms actually collect information, deal with children, or provide sufficient recourse to the consumer is less important than *cultivating the impression* that they do. Furthermore, strategic action may explain the relatively high conformance to the FIP category, *notice*. Companies want to provide a prominent link to their privacy policy and offer the impression of protection, even if the policy offers no real protection. For these companies, the privacy policy is a public relations tool. For example, the following represents the entirety of one financial company's privacy policy.

Zeta Company's long-standing commitment to safeguard the privacy of information our clients entrust to us is essential to our goal to be the world's first choice for financial services. Protecting the confidentiality and security of client information has always been an integral part of how we conduct our business worldwide. We pledge to continue to ensure that our global business practices protect your privacy.

The policy is linked to the homepage, promises privacy protection, but offers no specific plan on how protection is extended to the consumer.

**Strategic Action Validity Claims: Contextuality,**

Ngwenyama and Lee (1997) suggest that context is the most important validity claim related to strategic action. They argue that context determines whether a particular action is considered normal and acceptable or whether it is regarded as underhanded and deceptive.

In essence, online privacy policies exist within the *context* of the larger debate regarding information privacy and the tension that plays out among the actors. When a consumer accesses an online privacy policy, he or she is reading a document produced by a firm that has its own stakeholders and a legitimate profit motive. While a consumer may pay a price for less privacy online, he or she is likely to receive a benefit from providing personal information as well. Certainly, firms are expected to act in their own best interest. At the same time, society sanctions the existence of firms and requires that companies operate within a larger, societal context,

minimizing harm and maximizing contributions to society as a whole.

For decades, society has used the Fair Information Practices as a standard for assessing whether or not organizations are fairly handling individual personal information. When a firm uses a privacy policy to further its agenda at the consumer's expense, the original intention of a privacy policy is lost and society is damaged. On the other hand, when firms use the policy as a mechanism to protect consumers while simultaneously pursuing their own interest, then privacy policies are used for their intended purpose and society benefits.

In fact, much of the evidence for strategic action is demonstrated via the validity tests for the other social actions. For example, in the context claim for communicative action, the study shows that companies provide protection when it is not necessary (e.g., children and non-information collectors) and offering recourse that has little efficacy. With respect to the comprehensibility claim in communicative action, companies are stating the information practices, but obfuscating them through complicated verbiage and a misleading writing style. In the truthfulness claim in communicative action, companies do not really want others to know whether or not they are adhering to the policies. In instrumental action, firms limit the scope of their policies in order to limit their own liability. Finally, with discursive actions, companies are conforming to the letter of the law, but are not embracing the spirit of real privacy protection.

Each of these actions is consistent with the strategic interpretation of privacy policies as a mechanism of strategic action. In many cases, privacy policies actually enable privacy violations by providing the appearance of protection without any real substantive defense. Thus, FIP and privacy policies are being used as a smokescreen whereby actual privacy protection is limited and the focus shifts to enhancing the reputation of the company as a trustworthy business partner. Is this an acceptable strategic action, given the context of privacy policies and protection? The role of critical research is to illuminate these issues and put them in the public forum for debate.

### **Implications and Future Research**

This paper analyzes the online privacy policies of the *Fortune* 500, arguing that their primary purpose is not, in fact, to communicate information practices, as is commonly believed. Evaluating the four validity claims associated with communicative action, the

study finds that few policies comply with the communicative understanding. Actual communication may contain a blend of the four ideal types, but one category is likely to be dominant in any communication (Habermas, 1979; Habermas, 1984; Habermas, 1987). This study argues that strategic action is more dominant when compared to discursive, instrumental and communicative actions. It appears that many firms in the *Fortune* 500 use privacy policies as a public relations tool in order to cultivate the image of the firm as a trustworthy partner (Schwaig et al., 2004). The public relations perspective also accounts for some of the contextual difficulties in understanding privacy policies as communicative action.

Results of this study have important implications for future research and practice. First, future research should address the multiple social actions present in privacy policies. Researchers cannot afford to assume that the text of a given policy is associated with the privacy practices of the firm. Second, these conclusions point to a renewed dialogue regarding regulation of companies online. Previous regulation efforts have focused on controlling the privacy practices of companies, but a more important intermediate step might be to regulate and standardize the communication of those preferences.

Finally, future research should address the question of what is the appropriate context for strategic action. Of course, companies seek to present the best possible image to the public regarding their trustworthiness in protecting the privacy of the customer. Nevertheless, what disparity between image and actual protection is appropriate in this context? What actions constitute legitimate "spin" of the policies and where is the line where companies cross into deception? Previous research or public debate has not yet addressed these questions, and the primary contribution of the critical perspective of this research is to raise these very questions for later research and policy debate.

### **Conclusion**

Although the current state calls for self-regulation of online privacy practices, the results of this study indicate that firms are not in full compliance with federal standards. In fact, in adopting the perspective of online privacy policies as strategic action, the study argues that by using privacy policies as strategic rather than communicative action, companies adhere more to a *virtual reality of compliance*, as they appear to be more concerned about the existence of an information privacy policy than they do about its content and enforcement. The study provides several

interpretations for such observations, arguing that online privacy policies may serve a number of distinct and competing purposes other than simply protecting the privacy rights of consumers. A clear and consistent method for communicating compliance to Fair Information Practices has yet to emerge. A richer means for assessing the quality of online privacy policies and the role that they may play in firms is also needed. Industries that want to avoid future legislation need to develop effective communication and enforcement procedures that will satisfy both consumers and legislative bodies.

Finally, the study shows how Habermas's Theory of Communicative Action can be applied to analyze and uncover the true nature of online information privacy policies. The insights gained from the application of the theory should be useful for firms, governments and policy makers. Results should also provide researchers with interesting hypotheses for future research in the evolving information privacy debate.

## References

- Benassi, P. (1999). "TRUSTe: An Online Privacy Seal Program," *Communications of the ACM*, Vol. 42, No.2, pp. 56-59.
- Caudill, E.M. and Murphy, P.E. (2000). "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy and Marketing*; Vol.19, No.1.
- Culnan, M.J.(2000). "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy and Marketing*, Vol. 19, No. 1, pp. 20-26.
- Culnan and Milne, G.R. (2001). "The Culnan-Milne survey of Consumers and Online Privacy Notices. ([http://intra.som.umass.edu/georgemilne/PDF\\_files/culnan-milne.pdf](http://intra.som.umass.edu/georgemilne/PDF_files/culnan-milne.pdf))
- Federal Trade Commission. (2000). "Self-Regulation and Privacy Online: A Report to Congress", May, available at <http://www.ftc.gov/privacy>.
- Garfinkel, S.L. (2002). "Privacy matters," *CIO Magazine*.
- Hoffman, D.L., Novak, T. P. and Marcos, P. (1999). "Building Consumer Trust Online," *Communications of the ACM*, Vol. 42, No. 4, pp.80-85.
- Habermas, J. (1979). *Communication and the Evolution of Society*, Heinemann Press, London.
- Habermas, J. (1984). *The Theory of Communicative Action: Reason And Rationalization of Society (I)*, Beacon Press, Boston.
- Habermas, J. (1987). *The Theory of Communicative Action: Lifeworld And Social System (2)*, Beacon Press, Boston.
- Hann, I., Hui, K., Lee, T., Png, I.P.L.(2002). "Online Information Privacy: Measuring the Cost-Benefit Trade-off", Twenty-Third International Conference on Information Systems, pp. 1-8.
- Hirschheim, R and Klein, H.K. (1994). "Realizing Emancipatory Principles in Information Systems Development: The Case for ETHICS," *MIS Quarterly*, Vol. 18, No.1, pp. 83-109.
- Li, E.Y., R. McLeod and J.C. Rogers. (2001). "Marketing Information Systems in the Fortune 500 Companies: A longitudinal Analysis of 1980, 1990, 2000," *Information and Management*, Vol. 38, No. 5, pp. 307-322.
- Li, E.Y., R. McLeod and J.C. Rogers,(1993). "Marketing Information Systems in the Fortune 500 Companies: Past Present and Future," *Journal of Management Information Systems* Vol. 10, No. 1, pp. 165-192.
- Liu, C., and Arnett, K.P., (2002). "An examination of privacy policies in Fortune 500 web sites," *Mid-American Journal of Business*, Vol.17, No.1, pp.13-21.
- Lyytinen, K. (1992). "Information Systems and Critical Theory," in M. Alvesson and H. Willmott (eds), *Critical Management Studies*, Sage, Newbury Park, CA pp. 159-180.
- Lyytinen, K., and Hirschheim, R., (1988). "Information Systems as Rational Discourse: An Application of Habermas's Theory of Communicative Action," *Scandinavian Journal of Management*, Vol. 4, No. 112, pp.19-30.
- Lyytinen, K. and Klein, H.K. (1985), "The Critical Social Theory of Jorgen Habermas as a Basis for a Theory of Information Systems," in E. Mumford, R. Hirschheim, G. Fitzgerald and T. Wood-Harper (eds.), *Research Methods in Information Systems*, North Holland, Amsterdam, pp. 219-232.
- McLeod, R. and Rogers, J.C. (1982). "Marketing Information Systems: Uses in the Fortune 500," *California Management Review*, Vol. 25, pp. 106-118.
- Milne, G.R. and Culnan, M.J. (2002). "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys" *The Information Society*, Vol. 18, pp. 345-359.
- Miyazaki, A.D., and Fernandez, A. (2000). "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp.54-61.
- Mingers, J.C. (1981). "Towards an Appropriate Social Theory for Applied Systems Analysis: Critical Social and Soft Systems Methodology," *Journal of Applied Systems Analysis*, Vol. 7, No. 1, pp. 41-49.
- Ngwenyama, O.(1987). *Fundamental Issues of Knowledge Acquisition: Toward a Human Action Perspective of Knowledge Systems* unpublished Ph.D. dissertation, Watson School of Engineering,

State University of New York, Binghamton, NY.

Ngwenyama, O. (1991). "The Critical Social Theory Approach to Information Systems Problems and Challenges," in H. E. Nissen, H. Klein and R. Hirschheim (eds.), *Information Systems Research: Contemporary Approaches and Emergent Traditions*, North Holland, Amsterdam, pp. 267-280.

Ngwenyama, O.K. and Lee, A.S. (1997). "Communication Richness in Electronic Mail: Critical Social Theory and the Contextuality of Meaning" *MIS Quarterly*, pp. 145

Porter, A.M., (2000), "Buyers want Web Privacy," *Purchasing*, Vol.129, No.5, pp.22-25.

Schultze, U. and Leidner, D. (2002). "Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions." *MIS Quarterly*, Vol. 26, No. 3, pp.213-242.

Schwaig, K., Kane, G., and Storey, V.C. (2004). "Compliance to the Fair Information Practices: How are the Fortune 500 Handling On-line Privacy Disclosures?" Working paper, Kennesaw State University.

Smith, H. J. (1993), "Privacy Policies and Practices: Inside the Organizational Maze," *Communications of the ACM*, Vol. 36, No. 12, pp. 105-122.

Smith, H. J., Milburg, S.J., and Burke, S.J. (1996). "Information Practices: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, Vol.20, No.2, pp.167-196.

Stewart, K.A. and Segars, A.H. (2002). "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, Vol. 13, No. 1, pp. 36-49.

Swire, Peter P. (1997). "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in *Privacy and Self-Regulation in the Information Age*. Washington, DC: U.S. Department of Commerce, pp. 3-20.

Turner, E.C. and Dasgupta, S. (2003). "Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business

Organizations and Individuals," *Information Systems Management*, Winter, pp. 8-18.

U.S. Public Interest Research Group. (2000). as quoted in Hann et. al.

## About the Authors

**Kathy S. Schwaig** is an Associate Professor in the Michael J. Coles College of Business Administration Kennesaw State University in Atlanta, GA. She has research interests in information privacy, project management, knowledge management, and outsourcing. She has published in a variety of journals including *Information Systems Research*, *Journal of Management Information Systems*, *Communications of the ACM* and *Information and Organization*. Email: Kathy\_Schwaig@Coles2.kennesaw.edu

**Gerald C. (Jerry) Kane** is a doctoral student in Information Systems at the Goizueta Business School of Emory University. He has presented papers at the Academy of Management Conference, the North American Computational Social and Organization Science (NAACSOS) Conference, and the JAIS theory building workshop at ICIS. Jerry also holds an MBA in Computer Information Systems from Georgia State University. Email: jerry\_kane@bus.emory.edu

**Veda C. Storey** is Tull Professor of Computer Information Systems, J. Mack Robinson College of Business Administration Georgia State University. She has research interests in database management systems, intelligent systems, the Semantic Web, and ontology development. She serves on the editorial board of several journals including *Information Systems Research*, *Management Information Systems Quarterly* and *Data and Knowledge Engineering*. Email: Vstorey@gsu.edu