PATRICIA A. NORBERG, DANIEL R. HORNE,
AND DAVID A. HORNE

The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors

Impelled by the development of technologies that facilitate collection, distribution, storage, and manipulation of personal consumer information, privacy has become a "hot" topic for policy makers. Commercial interests seek to maximize and then leverage the value of consumer information, while, at the same time, consumers voice concerns that their rights and ability to control their personal information in the marketplace are being violated. However, despite the complaints, it appears that consumers freely provide personal data. This research explores what we call the "privacy paradox" or the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors.

With increasingly sophisticated technology, the effectiveness of collecting, storing, and analyzing vast amounts of consumer information has certainly increased, especially as related costs have fallen. Marketers who live by the adage "know thy customer" may view this progress as movement toward the desired state where knowledge of customers leads to ultra-efficient communication to exactly the right target audiences about product/service offerings, which perfectly match the needs and desires of those same groups (Moon 2000).

However, as marketers leverage the ability to collect and analyze ever-greater amounts of consumer information, serious concerns have arisen over the potential erosion of personal privacy (cf. Cavoukian and Hamilton 2002; Whiting 2002; Williams 2002). The popular press has featured privacy concerns as a major negative result of the "information age," and political forces have sought to transform consumers' felt deprivation into public policy initiatives. Consumers are constantly faced with the not-so-obvious trade-off between the desire for better products and services that are touted to be the result of more detailed customer profiles on the one

Patricia A. Norberg is an assistant professor in the Department of Marketing and Advertising, Quinnipiac University, Hamden, CT (patricia.norberg@quinnipiac.edu). Daniel R. Horne is an assistant professor of marketing at Providence College, Providence, RI (dhorne@providence.edu). David A. Horne is a professor of marketing at California State University – Long Beach, Long Beach, CA (dhorne@csulb.edu).

The Journal of Consumer Affairs, Vol. 41, No. 1, 2007
ISSN 0022-0078

hand and the privacy encroachment that such disclosure causes on the other.

Yet, for all the concern that people express about their personal information, which could be expected to drive one's intended and actual disclosure, our observations of actual marketplace behavior anecdotally suggest that people are less than selective and often cavalier in the protection of their own data profiles. Few studies have examined this discrepancy between individuals' intentions to protect their own privacy and how they behave in the marketplace. The purpose of this exploratory study is to investigate whether people say one thing (intend to limit disclosure) and then do another (actually provide personal details) during marketing exchanges. To that end, we report the results of two studies that demonstrate the existence of the privacy paradox and suggest that individuals' considerations of risk and trust help explain why it occurs. Additionally, a discussion of public policy is offered, with the goal of stimulating thoughts about how the desires of the public to maintain a sense of privacy may be preserved in an environment where privacy erosion seems inevitable.

BACKGROUND

That people are willing to trade personal information for perceived benefits is no surprise. For instance, a Web site that provides useful data may require the user to register in order to access the information. It is likely that economists and others would utilize an exchange framework to posit that the information the consumer receives from the Web site in this example is clearly of greater value than that of the information provided by the consumer to the site. Yet, this explanation seems less appropriate when we repeatedly witness people giving their phone numbers to clerks while engaged in simple cash transactions at a Sports Authority store. In this case, the benefit may be more difficult to ascertain. As O'Harrow noted in a recent book on surveillance and information collection, consumers "often willingly, even eagerly, part with intimate details of their lives" (2005, p. 54). While this seemingly asymmetric exchange, whereby the consumer receives limited value for providing information to a firm, has been noted (cf. Phelps, Nowak and Ferrell 2000; Han and Maclaurin 2002), few researchers have presented empirical evidence of the phenomenon (Sayre and Horne 2000; Spiekermann, Grossklags, and Berendt 2001).

The challenge in investigating actual disclosure and the impact thereon of privacy-related measures is threefold. First, privacy perceptions vary widely across populations and even within specific segments (Archer 1980; Culnan 1995; Nowak and Phelps 1992). A closely guarded secret

to one may be the chance for an appearance on *The Jerry Springer Show* for another. So too, certain domains of life are considered more private than others (Wasserstrom 1978; Phelps, Nowak, and Ferrell 2000). For example, Horne and Horne (1998) found that consumers were much more sensitive about the use of medical, financial, and family information than they were about their product and brand consumption or their media usage behavior. White (2004) makes the distinction between information, which when disclosed, causes a loss of privacy (control) and that which, when disclosed, causes embarrassment.

A second challenge faced in trying to understand privacy issues and phenomenon is the diversity of measurements used by previous researchers. Measures that have been used when examining privacy include attitudes toward privacy, concern for privacy, privacy-related behavioral intentions, and actual behavior, like disclosing personal information or taking affirmative steps to control information usage. This has resulted in some confusion regarding the implications that can be drawn from the literature from both behavioral and policy perspectives.

For example, large-scale studies, such as those conducted by Alan Westin throughout the 1990s (cf. Westin 1996), measured privacy in terms of "concern" about the current or future state of respondents' privacy. The concern measure provides some information about attitudes, though without dealing directly with the ambiguous nature of the term privacy. The studies by Westin and others (e.g., Smith, Millberg, and Burke 1996) have also examined concern to show that people have a range of attitudes toward privacy, which might either correlate with other factors like satisfaction with merchant offerings (e.g., Horne and Horne 1997), or which might result from certain antecedent conditions (e.g., Sheehan and Hoy 2000). For instance, Milne and Boza (1999) examined how concern related to trust and developed managerial implications, which suggested that increasing trust mitigated concerns.

While the difficulty in sufficiently measuring privacy attitudes is apparent, other researchers have attempted to look at privacy-related behavioral intentions. Here, the stated willingness to provide information or to take concrete steps to secure more privacy is investigated as a proxy for the actual behavior that consumers exhibit. For example, Schoenbachler and Gordon (2002) assess the willingness to disclose information as dependent upon the level trust in the organization, which is requesting the disclosure. Along a similar line, Bart et al. (2005) attempt to tie privacy, as a component of trust, to behavioral intention. Their construal of privacy, however, differed from other work in that they measure the perception of privacy-related activities on the part of the Web site (e.g., clarity of

privacy statement) rather than consumers' attitudes or concerns about privacy.

Finally, research into individuals' actual disclosure behaviors has been far more limited than that measuring concerns, attitudes, or behavioral intentions. Outside of the medical and related health services literature (e.g., Henderson et al. 2002; Potter 2002), studies dealing with methodological issues in data collection (cf. Dillman et al. 1996) and studies in psychology (Jourard 1971a, 1971b; Skotko and Langmeyer, 1977), very few efforts to track actual disclosure behavior are found. In marketing, investigations of actual disclosure behavior and of privacy attitudes and behaviors combined in one study are rare; however, we note two studies that do address these areas. Sayre and Horne (2000) examined actual disclosure and found consumers would freely trade personal information in exchange for small discounts at a grocery store. The widespread existence of retail and service loyalty programs indicates this practice covers many categories. In the other study, Spiekermann, Grossklags, and Berendt (2001) measured privacy attitudes and examined online behavior simultaneously, hypothesizing that the degree to which participants respond to information requests in an online shopping environment would be driven by their privacy concerns and preferences. Their study clustered participants into different aggregated privacy profiles based on willingness to provide personal information. In examining the degree to which the clusters differed in their personal information provision when exposed to an online shopping simulation, they found no significant differences in disclosure levels among the different privacy clusters. They did not, however, investigate factors that might explain why different privacy profiles respond similarly in a behavioral context.

CONCEPTUAL FRAMEWORK

In the privacy literature, several studies have focused on consumer willingness to provide information (e.g., Bart et al. 2005; Schoenbachler and Gordon 2002), but no study up to this point has focused on the degree to which these intentions might influence behavior and what other factors might affect the relationship. Even though only a paucity of direct evidence exists, several streams of research have examined consumer privacy and contribute to the development of the theoretical foundation from which the paradox may be explored. While much of the work in privacy has developed from a legal/rights basis (e.g., Schoeman 1984), *consumer* privacy work has concentrated on the idiosyncratic nature of the construct and on antecedent conditions that create greater or lesser feelings that the sphere of privacy is being encroached upon.

Two notable antecedents, risk and trust, have been investigated with respect to privacy concerns and intentions (Bart et al. 2005; Hoffman, Novak, and Peralta 1999; Horne and Horne 2002; Schoenbachler and Gordon 2002; White 2004) but less so with respect to actual privacy behaviors. We believe it is important to understand how these two factors might influence one's intention to disclose *and* one's actual disclosure behavior. As suggested by Milne and Boza (1999), we believe trust directly influences behavior. However, we also argue that risk considerations influence one's intention to disclose but are not strong enough to influence actual behavior. Therefore, we hypothesize that there is a significant difference between one's intention to disclose and actual disclosure because different frames of reference operate. When an individual is directly asked about intentions (willingness to provide personal information), risk is expected to significantly influence the response, but when an individual is in an actual disclosure situation (asked for information during a marketing exchange), trust as an environmental cue is expected to be relied upon and significantly influence response.

Figure 1 reflects how risk and trust might influence both behavioral intentions and actual behavior based on the suggestions of previous research. Figure 2, alternatively, is the conceptual model that underlies this research and reflects how we believe risk and trust truly operate with regard to both behavioral intention and actual behavior. Whereas the more traditional model shows that both risk and trust influence behavioral intentions that would then influence actual behavior, we argue that this is not the case. Instead, we argue that behavioral intention is not predictive

FIGURE 1
Conceptual Model of Disclosure Based on Previous Research

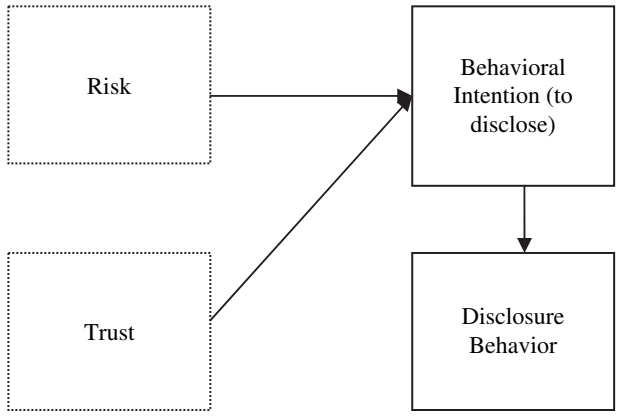
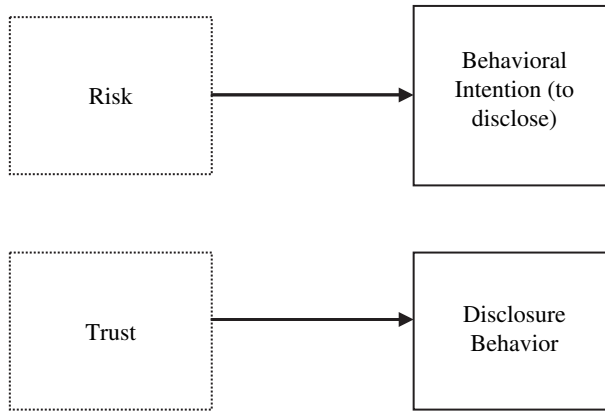


FIGURE 2
Conceptual Model—Privacy Paradox



of actual behavior because risk influences one's intention to disclose, while a trust heuristic operates in actual disclosure contexts. The following discussion clarifies our positions on trust and risk and the influence of each on intentions and actual disclosure.

Behavioral Intention

Behavioral intentions are formed based on the combination of an individual's attitude, subjective norms, and perceived control of an outcome (cf. Ajzen 1985). Previous findings show intention–behavior correlations of between .41 and .53 (O'Keefe 2002) with the measure being a better predictor of behavior when that behavior is voluntary. Three additional factors also have been shown to influence the strength of the relationship between intention and actual behavior: degree of correspondence between the measure of intention and the measure of behavior (Ajzen and Fishbein 1980), the temporal stability of intention (Ajzen and Fishbein 1980; Sheeran, Orbell, and Trafimow 1999), and the degree to which the behavior was planned (Gollwitzer and Brandstatter 1997; Sheeran, Orbell, and Trafimow 1999). O'Keefe (2002) and others (e.g., Bentler and Speckart 1979; Ouellette and Wood 1998) also argue that there may be other factors that influence behavior independently of intentions. Such factors might include routinization of behavior (Ouellette and Wood 1998) and/or the effects of heuristic processing or information selectivity in the decision process.

With respect to privacy, it is very possible that one's stated intentions are not reflective of their behavior because of factors that influence intention and behavior independently, like heuristic processing and routinization of behavior. For example, one's evaluation of an organization's trustworthiness might be used as a means of evaluating how much and what type of personal information one will give up to that organization. Additionally, the constant and routine requests for information (e.g., postal codes, phone numbers) by commercial interests coupled with the relatively small level of realized losses (FTC 2003) incurred from responding to these requests appear to lead to consumers that readily supply information, potentially due to low perceived risk, even though inquiries regarding intentions to disclose indicate otherwise.

Privacy research also suggests that social desirability bias could contaminate one's responses to "willingness to disclose" personal information items in such a way that behavioral intentions would not be predictive of actual disclosure behavior (Milne 1997). There is some evidence, however, that such a bias might not be of significant concern to researchers in this area. Norberg (2004) compared what a person said they were willing to disclose to what that person believed others typically disclose in a marketing setting and found no significant difference. Thus, it appears that at a minimum, people think that their own disclosure behavior is no different from others.

Risk

Risk, on a general level, has been defined previously as uncertainty resulting from the potential for a negative outcome (Havlena and DeSarbo 1991), and one's evaluation of risk is influenced by the perceived likelihood of the negative event occurring as well as the perceived severity of that event (Peter and Tarpey 1975). Risk has also been broken down into its dimensionality or type of risk that contributes to an overall perception of risk (Deering and Jacoby 1972; Jacoby and Kaplan 1972).

Previous research has shown that risk influences perceptions of privacy. *Perceived* disclosure consequences (White 2004) are reflective of one's perception that negative outcomes may be greater than potential benefits when personal information is disclosed. These negative perceptions may affect individuals emotionally, materially, or even physically (Moon 2000). For instance, a past medical condition, if disclosed, may preclude future medical insurance coverage or even employment that could lead to a negative impact on an individual's health and/or financial status. While disclosure of this nature may significantly impact the individual in a

negative manner, negative outcomes may also relate to the deterioration of perceived self-image from the discomfort or embarrassment that something an individual wishes to remain secret becomes publicly known. Horne and Horne (2002) showed that concern about these potential negative outcomes had a relatively greater impact on perceptions of privacy than did the level of trust in the organization. Although it appears that consumer concern is certainly driven by risk perceptions, as these studies suggest, today's marketing environment and the lack of consumer recognition of privacy breaches should make one question the effects of risk perceptions on actual behavior.

Trust

Trust has been defined previously in a variety of ways. For example, Moorman, Deshpande, and Zaltman (1993) defined trust as a willingness to rely on an exchange partner. In consumer privacy and in online contexts, trust has been measured directly (Garbarino and Lee 2003; Schoenbachler and Gordon 2002) as well as indirectly operationalized as a company's reputation (Andrade, Kaltcheva, and Weitz 2002). While noting that trust operates differently in online and offline environments, Bart et al. (2005) develop a substantial list of factors impacting online trust.

When trust is made salient to consumers who are asked about their willingness to provide personal information to marketers, negative privacy perceptions appear not to be reflective of their willingness to provide personal information. Both Schoenbachler and Gordon (2002) and Hoffman, Novak, and Peralta (1999) found that higher levels of trust were related to increased willingness to provide personal information. Also related to trust, Earp and Baumer (2003) examined the effects of brand name status and found that consumers expressed a higher willingness to disclose personally identifying and financial information to well-known companies. Milne and Boza (1999) examined the impact of trust on a consumer's sense of privacy and found that trust was a better means of managing customer data over attempts to reduce concern about privacy. Similarly, Cranor, Reagle, and Ackerman (1999) demonstrated that the level of intended disclosure of personal information was positively related to the level of trust for the organization. Bart et al. (2005) also find a relationship between the privacy component of trust and behavior intention, though their measure of intention addresses intention along other dimensions (i.e., purchase intention, willingness to provide word-of-mouth communications) as well as one element of information disclosure (willingness to register).

These findings suggest that organizations may considerably lessen privacy concerns by establishing trusting relationships with consumers, and indeed marketers may leverage environmental cues to make consumers feel comfortable during commercial exchanges. Moreover, consumers typically use heuristics to guide behavior (Bettman 1979; Scholz and Lubell 1998) and will utilize cues in the environment, such as personal characteristics (Allport 1954) or design elements for a Web site (Freeman and Spyridakis 2004) to infer trust. The use of trust as a heuristic (Scholz and Lubell 1998) in disclosure situations might significantly shorten the disclosure decision-making process, thus circumventing effortful cognitive processing.

Although it is of significant value for organizations to understand that trust building is important in establishing relationships with consumers, little is known about the effects of trust on willingness versus actual disclosure, given a particular marketing exchange context. The studies discussed above clearly indicate that trust perceptions influence one's feelings about privacy (where more trust leads to less privacy concern). However, we believe that in a real exchange situation, where environmental cues used by the organization to establish trust are more salient, consumers are more influenced by trust than their willingness indicators would suggest. This may make consumers very vulnerable to unreliable sources that create cues to instill trust in order to carry out unethical business practices.

HYPOTHESES

Although consumers seem to be concerned about their privacy as reflected in their intentions to disclose (e.g., measured via "willingness to provide information"), anecdotal evidence suggests their behaviors diverge from their intentions to disclose personal details. However, this "gap" has never been measured. The frequent requests for information in commercial interactions and the relatively small level of realized losses incurred from responding to these requests lead to consumers who readily supply information, even though inquiries regarding intentions to disclose indicate otherwise.

H1: Individuals will *actually* disclose a significantly greater amount of personal information than their stated intentions indicate.

When asked about willingness to disclose (behavioral intention), perceived risk of disclosing personal information is expected to be salient. Individuals typically have privacy concerns that are formed based on

external sources of information (e.g., the media), where the external environment highlights the negative issues associated with privacy or, more specifically, the risks apparent in personal information access and availability. This may drive the intention to disclose because questions asked prime the respondent. For example, the media's coverage that "identity theft" is reputed to be the fastest growing crime in the United States (Knapp 2004), in addition to credit card ads emphasizing identity protection needs, reflects the negative aspects of privacy breaches that may influence privacy concern. Thus, when individuals are asked about such concerns directly, or about what personal information they would be willing to disclose to marketers, consumer reliance on privacy stereotypes and the ease of accessing negative information from memory will influence their intention responses.

H2: Risk perceptions will have a significant negative impact on individuals' *stated intentions* to disclose personal information.

During actual disclosure situations, salient environmental cues will likely be relied upon when making disclosure decisions. As marketers strive to create exchange environments that are perceived to be trustworthy, individuals are likely to infer trust from the marketers' cues as they rely on heuristic processing (cf. Bettman 1979; Scholz and Lubell 1998) in these more routine disclosure situations. Thus, trust is expected to influence personal information disclosure more in actual situations regardless of stated intentions.

H3: Trust perceptions will have a significant positive impact on individuals' *actual* personal information disclosure.

METHOD

Study Design

To compare disclosure intentions to actual disclosure, two studies were conducted and both used a repeated-measures design, whereby individuals were asked their willingness to disclose specific pieces of information in Phase 1 of each study and then several weeks later were asked to actually provide the same specific pieces of information to a market researcher in Phase 2. *T*-tests were used to compare the two measures (H1). Additionally, in the second study, regression was used to examine the impact of perceived trust and perceived risk on intentions and actual behavior

(H2 and H3). The studies took place in classroom settings, and the appropriate informed consent procedures were followed.

Independent Variable

Scenarios were used to depict a particular marketing context to which subjects were asked to respond. Scenarios are further described in the Study 1 and Study 2 sections and appear in the appendix.

Dependent Variables

Dependent variables were operationalized as follows:

Behavioral Intention (Phase 1): Total number (sum) of personal items that subject identified they would provide to a marketer.
Actual Disclosure (Phase 2): Total number (sum) of personal information items subjects supplied. The items requested were identical to those in the Behavioral Intention questionnaire.
Perceived Risk: One-item measure of how risky subjects felt it was to provide information to the marketer, using a 7-point semantic differential scale anchored by "not at all risky" and "very risky."
Perceived Trust: Three-item scale of how trustworthy, honest, and sincere subjects felt the company was on three 7-point Likert-scale items anchored by "strongly disagree" and "strongly agree."

STUDY 1

The goal of Study 1 was to examine initially whether or not we could provide support that the privacy paradox actually exists. A sample of twenty-three part-time, evening program graduate students at a university in the Northeast participated in the experiment. The age range of the sample was 22–40, and the gender split was even. Subjects were initially asked to respond to behavioral intention questions related to disclosing seventeen pieces of personal information, given a particular marketing scenario that was pretested as described below. These subjects then were asked twelve weeks later to actually provide the same seventeen pieces of personal information to a confederate claiming to represent a commercial enterprise. Thus, individual responses from Phase 1 of each study could be directly matched to the individual responses in Phase 2. See Appendix 1 for the selected scenario and information items.

Pretests

Four marketing scenarios were pretested with the goal of obtaining one scenario that would constitute a believable marketing program for the behavioral condition for an adult group. These scenarios were presented to forty-three graduate students who were asked to rate how trustworthy and risky they felt each situation was with respect to providing personal information. The situation that was selected for the first study, based on risk and trust ratings, was that of a large bank that was introducing a graduate student credit card. The bank scenario best demonstrated the characteristics the researchers were seeking—a higher level of trust in the bank coupled with some perception of risk (e.g., providing financial data). The researchers felt this scenario would also be highly believable in Phase 2 where actual data were being collected by "a large bank."

Phase 1

Subjects completed a pencil-and-paper questionnaire to capture respondents' willingness to provide personal information to a large bank. The questionnaire stated that the bank would pay a $20 incentive for providing the information. The compensation was included in the scenario to heighten the perceived benefit of disclosure in the condition, given that we were measuring behavioral intention. Respondents were asked to check off from a list of items items they would be willing to provide about themselves. The questions were embedded in a larger survey to add distraction and contribute to the memory decay that was important for the administration of the Phase 2.

Phase 2

Twelve weeks following the collection of the intention data, respondents were asked to engage in actual personal information disclosure. The goal of the temporal separation of the two phases was to ensure that participants did not remember their involvement in the first phase. Specifically, in the execution of Phase 2, a confederate visited campus under the guise of carrying out research for a pilot program for a bank. The confederate informed the participants that the bank program was being targeted toward graduate students, and thus the company was visiting college campuses. Next, the situation taken directly from the scenario from Phase 1 was described. The only modification to the scenario in Phase 2 was the lack of monetary incentive—the Phase 1 scenario described some compensation for the

information sought, whereas no incentive was offered for the actual provision of information. The monetary incentive was excluded in Phase 2 to reduce motivation for disclosure and to provide a stronger test.

The confederate distributed pencil-and-paper data collection booklets. The students were asked to complete the booklets (provide personal information) and were instructed to leave items blank if they did not want to provide data, instead of filling in erroneous information. By informing subjects that they could omit information they were not comfortable providing, we attempted to minimize the risk of information quality confounds. Although one might argue that the classroom setting would have a positive influence on actual disclosure, we believe this is consistent with any environment where marketers utilize cues to influence consumers' perceptions of trust (as previously discussed), which positively influences exchanges. We did not, however, want to create an environment that was overly trustworthy, and thus it was communicated to participants that the "market researcher" was not acquainted with the faculty of the particular school but was visiting a variety of classrooms on campuses across the region.

After taking the survey, subjects were debriefed. At this point, the actual identity of the confederate was disclosed, and it was ascertained whether the subjects retained a memory trace of that earlier task. Discussion demonstrated that, until prompted to remember, none of the subjects had recalled the Phase 1 task while participating in Phase 2. The researchers also discussed the true nature of the study with participants, and participants were told that they could keep the booklet that they just completed if they did not wish to continue with the study.

Data Coding

Because the researchers were collecting both identifying and potentially sensitive personal data in Phase 2 of the experiments, care had to be taken during data coding. Responses were recorded and coded by the researcher who was unfamiliar with the particular subject pool. All information items were coded only as either provided (1) or not provided (0), while actual values of information items were not recorded for analysis. Note, however, that actual values were checked by the coding researcher in order to identify any blatantly bogus data (e.g., Donald Duck in the Name Field).

Study 1 Results

To add support that the privacy paradox exists, Phase 1 and Phase 2 records were matched, and the number of items respondents said they were

willing to disclose in Phase 1 was compared to the number of items they actually disclosed in Phase 2. The *t*-tests showed that willingness to disclose (mean = 8.70, SD = 4.49) was significantly different from actual disclosure (mean = 14.75, SD = 2.22), with $t = -7.63$, $p < .000$, and effect size measured by partial eta square = .75. The findings strongly support our argument in that individuals provide significantly greater amounts of personal information than they say they will. Thus, H1 was supported.

STUDY 2

In Study 2, undergraduate students were exposed to one of two disclosure situations that were pretested, as described below. Subjects were initially asked to respond to behavioral intention questions related to disclosing sixteen pieces of personal information (Phase 1). These subjects then were asked seven weeks later to actually provide the same sixteen pieces of personal information to a confederate claiming to represent a commercial enterprise (Phase 2). Trust and risk were also measured in both phases of the Study. See Appendix 2 for scenarios and information items, and Appendix 3 for and trust/risk measures.

Pretests

In preparation for the experiment, four marketing scenarios were pretested with the goal of selecting two scenarios that respondents felt differed significantly with respect to trustworthiness. By using two scenarios that differed on trust, we were given the opportunity to measure the degree to which trust, even for a situation that was deemed less trustworthy, could affect the participants' behavioral responses to personal information requests and their actual disclosure. Measures appear in Figure 3.

In the pretest, the proposed scenarios were presented, during three rounds, to a total of eighty-three undergraduate students from two colleges

FIGURE 3
Measurement Model

Scenarios	**Measurement 1 (Phase 1)**	**Measurement 2 (Phase 2)**	**Information Items**
High-Trust Scenario (Bank)	Behavioral Intention to Disclose Perceived Risk Perceived Trust	Actual Disclosure Behavior Perceived Risk Perceived Trust	7 highly sensitive 7 moderately sensitive 2 low sensitive
Low-Trust Scenario (Pharma)	Behavioral Intention to Disclose Perceived Risk Perceived Trust	Actual Disclosure Behavior Perceived Risk Perceived Trust	7 highly sensitive 7 moderately sensitive 2 low sensitive

in the Northeast. The students were asked to rate how trustworthy they felt each scenario was with respect to providing personal information. Based on high and low perceived trust scores (Table 1), two of the four scenarios were selected for the actual experiment. The low-trust scenario involved disclosing information to a pharmaceutical company with a poor reputation and the high-trust scenario involved disclosing information to a large reputable bank.

Phase 1

As part of a larger pencil-and-paper questionnaire that included several distracter tasks, one of the two scenarios (pharmaceutical company/bank) was presented to respondents. They were asked to read the scenario and check off from the list of sixteen personal information items those pieces of information that they would be willing to provide to the company described in exchange for $20. Subjects then responded to the trust and risk perception scale items with respect to disclosing information to either the pharmaceutical company or the bank. Twenty-eight subjects responded to the pharmaceutical scenario and forty subjects responded to the bank scenario, for a total sample of sixty-eight individuals in Phase 1.

Phase 2

Seven weeks following the collection of data in Phase 1, the subjects who participated were visited in Phase 2 by a confederate posing as a market researcher representing a commercial company in the same manner as in Study 1. This confederate described the bank credit card or pharmaceutical program that was exactly like the scenario in Phase 1, with the only modification in Phase 2 being a lack of monetary incentive.

TABLE 1
Study 2 Pretest Results: Mean (SD) Trust Ratings

N	Scenario	Mean (SD)	*t*-Test Bank versus Pharma (trust)
55	Health club	4.73 (0.91)	$t = 3.48$, $p = .001$
	Bank	4.58 (1.21)	
	Pharma	3.88 (1.10)	
	Reality TV show	3.92 (1.12)	
28	Health club	4.43 (0.81)	$t = 4.95$, $p = .000$
	Bank	4.86 (0.90)	
	Pharma	3.43 (1.05)	

Data collection booklets were distributed, and the subjects were asked to complete the booklets (provide personal information). Respondents were instructed to leave items blank if they did not want to provide information instead of filling in erroneous information. To ensure that the subjects who participated in Phase 1 of the project did not retain a memory trace of that task, and to discuss the true nature of the study with participants, debriefing took place after Phase 2 similar to the debriefing during Study 1. As was the case in Study 1, until prompted, none of the subjects had recalled the scenarios from Phase 1 while participating in Phase 2. Data coding followed the same procedure as in Study 1.

Study 2 Results

Not all subjects attended both sessions, so fifty-five completed Phase 2 questionnaires were matched to Phase 1 questionnaires (thirty-two participants in the bank condition and twenty-three participants in the pharmaceutical condition). Because two different scenarios were used in Study 2, personal data items differ somewhat by scenario to ensure that the data requested were appropriate to the scenario. However, the data items selected are expected to be subjective equivalents (Cranor, Reagle, and Ackerman 1999; Norberg 2004) and therefore scenarios can be analyzed together. Because multiple tests on the same data were performed, a Bonferroni adjustment was made to the significance level, and a significance level of .01 was used for analysis.

Scale reliability was checked for the 3-item trust measure. Cronbach's alpha for trust in Phase 1 was .96 and in Phase 2 was .95. The *t*-tests were then performed to check the manipulation of trust in the scenarios, and the mean differences between high and low trust were significant (Table 2).

The first and primary focus of the study was to provide evidence that the privacy paradox, or the difference between information actually provided as compared to a willingness to provide, exists (H1). Therefore, the number

TABLE 2
Study 2 Condition Manipulation Check

Phase/Scenario	Mean (SD) Trust	*t*-Statistic	Significance
Behavioral intention		3.754	.000
Bank	4.60 (1.27)		
Pharma	3.39 (1.11)		
Actual behavior		6.514	.000
Bank	5.64 (0.85)		
Pharma	4.01 (0.84)		

of items that respondents said they were willing to provide in Phase 1 (behavioral intention) was compared to the number of items they actually provided in Phase 2 (actual behavior). As indicated in Table 3, *t*-tests showed that willingness to disclose (mean = 10.49, SD = 3.10) was significantly different from actual disclosure (mean = 15.16, SD = 1.15), with $t = -10.02$, $p < .001$. The difference in disclosure was also analyzed independently for both the bank and the pharmaceutical conditions. Total items intended versus actual disclosure was significantly different for each condition, with $t = -7.41$ ($p < .000$) and $t = -6.66$ ($p < .000$) respectively. H1 was supported as respondents did provide significantly greater amounts of personal information than they say they would.

Next, the risk–intention, risk–actual disclosure (H2) and trust–intention and trust–actual disclosure (H3) relationships were examined using regression (Table 4). Risk was tested separately from trust because the two measures exhibit multicollinearity when tested together. According to Hair et al. (1998), if two measures are conceptually different but are likely to covary, then the measures can be regressed separately to remedy the multicollinearity problem.

The regression result for the risk–intention to disclose relationship was found to be significant ($F = 6.973$, $p = .011$), and the result for the risk–actual disclosure relationship was found to be not significant ($F = 2.075$, $p = .157$). Thus, we found support for H2 as it does appear that risk is salient when asking for behavioral intention responses but is less so in actual disclosure situations. All relationships were in the expected direction.

With regard to H3, it was expected that trust would have a greater positive influence on disclosure behavior than it would on intention to disclose. The respondents' answers to the 3-item trust scale were used to measure the relationships. None of the relationships between trust and the dependent variables were significant.

The lack of support for H3 is contrary to some previous findings that trust significantly impacts an individual's *willingness* to provide personal

TABLE 3
Study 2 Hypotheses 1 Results: Differences between Intended and Actual Disclosure

Condition	Mean (SD)—Items Willing to Disclose (Phase 1)	Mean (SD)—Items Actually Disclosed (Phase 2)	*t*-Statistic	Significance	Effect Size
Overall	10.49 (3.10)	15.16 (1.15)	−10.02	$p = .001$	.65
Bank	10.38 (3.17)	15.13 (1.21)	−7.41	$p = .000$	.64
Pharma	10.65 (3.07)	15.22 (1.09)	−6.66	$p = .000$	.67

TABLE 4
Study 2, Hypotheses 2 and 3: Regression Results for Risk and Trust Relationships

IV	DV	R^2	df	Beta	F	p
Risk	Intention to disclose	.118	53	−.344	6.973	.011
	Actual disclosure	.045	45	−.212	2.075	.157
Trust	Intention to disclose	.026	54	.162	1.428	.237
	Actual disclosure	.011	45	−.104	.486	.489

Note: IV = "Independent Variable" and DV = "Dependent Variable".

information but is consistent with the findings reported by Horne and Horne (2002). It is possible that because the companies were unknown to the respondents (no company names were provided) in this study, trust cues were not strong enough to impact one's actual disclosure. Further, trust and risk may interact in that higher levels of risk may require higher levels of trust for disclosure to take place. This might be the case under certain conditions, where the disclosure context and the type of data (sensitive/personal versus less sensitive/personal) being requested and should be taken into account. Based on the mixed-trust findings, we suggest that trust may not *always* operate but may be more likely to operate under extreme conditions, where very sensitive data or, conversely, innocuous data are being requested from very well-known companies or, conversely, companies that are easily identified as "questionable." Yet, there are many instances where consumers are being asked for information that is only "somewhat sensitive" and are engaging in discourse with companies that do not fit either of the "well-known" or "suspicious" categories. Under these conditions, trust might be difficult to assess and therefore personal disclosure behavior may be better explained by factors other than trust.

DISCUSSION

The purpose of this exploratory research was to attempt to confirm and explain a particular behavior that the researchers had repeatedly witnessed in the marketplace. However, caution must be exercised in trying to generalize from this work into different less-controlled settings. While we attempted to control a number of outside variables and to provide realistic scenarios, our findings may be, in part, artifacts of the data collection environment. Even though we believe the classroom setting operated as any other environmental cue, it is possible the setting created too much trust. This overabundance of trust in their educational institution may have given subjects greater confidence that their information would not be used in an inappropriate manner.

Additionally, even though we informed subjects that they should leave information items blank as opposed to entering erroneous data when they were not comfortable supplying personal answers, there exists the possibility that data quality may vary. While inspection of the data for blatant misrepresentations was performed, each response was simply recorded as either provided or not.

We hypothesized that people *say* that they are less willing to provide personal information to marketers than they actually provide when a marketer directly requests such information from them because perceptions of risk and trust are activated differently when intention measures are taken as compared to actual disclosure settings. In the two studies reported here, we found that the level of actual disclosure significantly exceeded individuals' intentions to disclose. The difference in level of information provided in all information categories (personally identifying, financial, preferences, demographic, etc.) emphasizes the need to put more research effort into understanding actual behavior. It appears that, in the realm of privacy, behavioral intentions may not be an accurate predictor of actual behavior and other explanations should be sought.

Demonstrating the existence of the Paradox itself is but a precursor to the real challenge to discover the antecedent conditions that more fully explain why this phenomenon exists and how these discrepancies between attitudinal measures, measures of intention, and behavior can be addressed. The research reported herein provides evidence that, under certain conditions, even people with negative perceptions about disclosing certain personal information will actually produce the information when directly requested. The ability to generalize from this work and the development of information and educational efforts that will help consumers make informed decisions about their provision of personal data will only result if individual antecedents are identified and tested. Contextual factors such as the physical setting, social factors reflecting the relationship between the individual and the person(s) or institution collecting the information, and cognitive factors all may help explain in part the findings presented. Moon's (2000) work with intimate disclosure to a computer "being" is an interesting branch of this type of work.

To examine why the gap exists, we hypothesized that risk would significantly influence individuals' behavioral intentions toward providing personal information, while trust would significantly influence their actual behavior. We found support in Study 2 that risk is activated and significantly influences individuals' intentions to provide, while not influencing their actual behavior. However, we did not find support for trust operating as expected. The influence of trust on actual behavior, as opposed to the

influence on intended behavior that has been the focus in many of the past studies, is still a question. Since there is little research that examines risk and trust in tandem, here is an opportunity to extend this work and develop a better understanding of these two underlying mechanisms. Future research should be geared toward understanding trust and risk interactions not only in extreme cases (well known vs. suspicious companies and very personal vs. innocuous data requests) but also in those more ambiguous cases. Such research would help bring previous findings and the findings in this study together. However, boundary conditions that help explain the independence or interaction of trust and risk are not fully explanatory. Future research, on a practical level, must examine how factors such as the physical environment, the media of data collection and responses to human interaction impact our assessment of trust and risk.

Understanding why consumers respond the way they do is of critical importance in this arena where public policy relies upon consumer attitudinal-based perspectives. Surveys of consumers that show a sense of increasing erosion of personal privacy might spur calls for legislative reactions. Yet, all the while, anecdotal evidence and our study suggest consumers nonchalantly provide their personal information on a regular basis. In light of this, should policy responses be directed at increasing salience through creating awareness of the potential harm? Or should these decisions be removed largely from the consumer's volition through strict proscriptions against data collection? Research attention could be directed toward the effects of awareness/educational initiatives that might better align consumer concern for privacy with their marketplace behaviors. As O'Keefe (2002) noted, explicit planning influences the relationship between intention and disclosure. Consumer-based educational programs might help direct consumers away from shortcut heuristic processing by influencing consumer involvement in their own disclosure decision processes. At the same time, increased consumer awareness might lead consumers to actions that will force commercial parties to improve their offers in exchanges involving consumer information.

CONCLUSIONS

Consumer privacy has become a "front burner" issue for policy makers over the past decade as countless tales of personal misery made this topic a prime candidate for a myriad of proposed legislative action. At the same time, the current trajectory is certainly for more versus less collection and use of personal information with consumers increasingly feeling like they have "no place to hide." While policies struggle to keep pace with new

technologies, it is fair to question the reliance solely on protective legislation that may be ineffective when individuals willingly disclose personal information. According to Rosenberg, "the best and most effective way to control use of information, without interfering with the conduct of others, is to prevent it from ever coming into others' hands" (2000, p. 84). It would appear, however, that despite protestations to the contrary, consumers are the conduits of much of this information.

From a policy maker's perspective, this creates a dilemma: should consumers be protected from their own chosen behaviors? Should regulatory efforts mandate how information is collected to obviate the need for consumers to monitor their own behavior? Our sense is that current movements toward permission-based data collection and usage may address some of the issues raised herein. However, further study in the privacy area is still warranted before additional significant policy changes are made.

There must be the realization that, unless consumers make the effort to truly understand what they are granting permission to, and to whom they are giving their personal information, their sense of personal privacy will continue to deteriorate. Especially, as people expand their usage of data-rich transaction channels such as the Internet, the need to comprehend where the data go increases dramatically. We have only to look to the usage of "privacy policy" on various Web sites as an example. These are generally ignored or are imbued with many positive, though nonexistent, attributes by virtue of their mere presence on the site (Milne, Rohm, and Bahl 2004; Miyazaki and Krishnamurthy 2002). The danger is that public policy decisions that only address part of the problem will be made. These may negatively impact commercial entities' abilities to deliver the goods and services desired by their markets without creating a concomitant real benefit to consumers. Enlisting consumers as the first line of defense to protect their own privacy may well emerge as the most efficient means to ease everyone's concerns with the data collection race that quickens all around us.

APPENDIX 1

Graduate Scenario

A large bank, with an excellent reputation for ethical programs, is developing a "Graduate Student Supreme" credit card that will give a percentage of purchase prices back to the student in gift certificates to the college bookstore and local restaurants, movie passes, and travel vouchers.

As part of the bank's analysis of whether to go forward with this program, they are doing research into this student market. They have acquired a list of students and contacted you to take part in the research. You would be compensated $20.

From the following list, please check which pieces of information you would be willing to provide:

- ☐ Name
- ☐ Experience with applying for credit (number of credit cards, loans, etc).
- ☐ E-mail
- ☐ Gender
- ☐ Phone
- ☐ Attitudes toward lending money to friends
- ☐ Address
- ☐ Opinions regarding the use of credit cards
- ☐ Monthly purchases in categories like food, clothing, entertainment, going out
- ☐ Age
- ☐ Hobbies
- ☐ Attitudes toward saving money
- ☐ Make, model, and year of car owned
- ☐ Dining preferences (types of food like American, Italian, Sandwiches, Tapas, etc.)
- ☐ Individual monthly income
- ☐ Total family income
- ☐ Preference for shopping online for categories like music, books, clothing, travel

APPENDIX 2

High-Trust Scenario

A large bank, with an excellent reputation for ethical programs, is developing a "Student Supreme" credit card that will give a percentage of purchase prices back to the student in gift certificates to the college bookstore and other businesses located on campus. As part of their analysis of whether to go forward with this program, they are doing research into this student market. They have acquired a list of students and contacted you to take part in the research. You would be compensated $20.

From the following list, please check which pieces of information you would be willing to provide:

- ☐ Experience with applying for credit (number of credit cards, loans, etc.)
- ☐ E-mail
- ☐ Gender
- ☐ Phone
- ☐ Attitudes toward lending money to friends
- ☐ Address
- ☐ Opinions regarding the use of credit cards
- ☐ Monthly purchases in categories like food, clothing, entertainment, going out
- ☐ Age
- ☐ Hobbies
- ☐ Attitudes toward saving money
- ☐ Make, model, and year of car owned, if any
- ☐ Dining preferences (types of food like American, Italian, Sandwiches, Tapas, etc.)
- ☐ Monthly income
- ☐ Parents' income
- ☐ Preference for shopping online for categories like music, books, clothing, travel

Low-Trust Scenario

A pharmaceutical company, which has had some recent high-profile failures, has invested significant resources in developing a drug intended for the over-the-counter market, which, when taking after drinking, limits the negative impacts associated with hangovers (i.e., fatigue, headache, nausea). As they design a marketing strategy for this product, they are collecting research to evaluate if and how it can be successfully introduced. In order to collect the data, they are asking students to sign up to take part in the study. Once accepted, students are asked to fill out a questionnaire (in exchange for $20).

From the following list, please check which pieces of information you would be willing to provide:

- ☐ Religious beliefs
- ☐ Address

- ☐ Personal health history
- ☐ Monthly income
- ☐ Attitudes on drinking and driving
- ☐ Attitudes toward laws and regulations on drinking/alcoholic consumption
- ☐ Alcohol consumption (frequency, location, and amount of drinking)
- ☐ Shopping or setting preferences for categories like food, clothing, health, and beauty items
- ☐ Prior experience with hangovers (frequency, symptoms, degree of severity of symptoms, duration of symptoms)
- ☐ Phone
- ☐ Gender
- ☐ Monthly purchases in categories like health and beauty, over-the-counter medicines (such as for headaches, indigestion, or allergies)
- ☐ Dining preferences (like American, Italian, Sandwiches, Tapas, etc.)
- ☐ E-mail
- ☐ Hobbies
- ☐ Age

APPENDIX 3

Trust Questions (rated on 7-point Strongly Disagree to Strongly Agree Scale)

This company is trustworthy
This company is honest
This company is sincere

Risk Questions (rated on 7-point Semantic Differential Scales)

In general, to what degree do you feel it is risky for people to provide the personal information requested to this company? (not at all risky to very risky)

REFERENCES

Ajzen, Icek. 1985. From Intentions to Actions: A Theory of Planned Behavior. In *Action Control: From Cognition to Behavior*, edited by J. Kuhl and J. Beckmann (11–9). New York: Springer-Verlag.

Ajzen, Icek and Martin Fishbein. 1980. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Allport, Gordon W. 1954. *The Nature of Prejudice*. Cambridge, MA: Addison-Wesley.

Andrade, Eduardo B., Velitchka Kaltcheva, and Barton Weitz. 2002. Self-Disclosure on the Web: The Impact of Privacy Policy, Reward and Company Reputation. In *Advances in Consumer Research*, edited by Susan M. Broniarczyk and Kent Nakamoto, vol. XXIX (350–353). Valdosta, GA: Association for Consumer Research.

Archer, Richard L. 1980. Self-Disclosure. In *The Self in Social Psychology*, edited by Daniel M. Wegner and Robin R. Vallacher, 183–204. New York: Oxford University Press.

Bart, Iakov Y., Venkatesh Shankar, Fareena Sultan, and Glen L. Urban. 2005. Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large Scale Exploratory Empirical Study. *Journal of Marketing*. 69 (October): 133–152.

Bentler, Peter M. and George Speckart. 1979. Models of Attitude-Behavior Relations. *Psychological Review*, 86 (5): 452–464.

Bettman, James R. 1979. *An Information Processing Theory of Consumer Choice*. Reading, MA: Addison-Wesley Publishing.

Cavoukian, Ann and Tyler Hamilton. 2002. Whither Privacy, post–9/11? *Toronto Star*, September 9, 2002: D3.

Cranor, Lorrie Faith, Joseph Reagle, and Mark S. Ackerman. 1999. Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. AT&T Labs-Research Technical Report TR99.4.3. http://www.research.att.com/.

Culnan, Mary J. 1995. Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing. *Journal of Direct Marketing*, 9 (Spring): 10–19.

Deering, Barbara J. and Jacob Jacoby. 1972. Risk Enhancement and Risk Reduction as Strategies for Handling Perceived Risk. In *Proceedings of the Third Annual Conference of the ACR* (404–416). Association for Consumer Research.

Dillman, Don A., Eleanor Singer, Jon R. Clark, and James B. Treat. 1996. Effects of Benefits Appeals, Mandatory Appeals, and Variations in Statements of Confidentiality on Completion Rates for Census Questionnaires. *Public Opinion Quarterly*, 60 (Fall): 345–375.

Earp, Julia B. and David Baumer. 2003. Innovative Web Use to Learn about Consumer Behavior and Online Privacy. *Communications of the ACM*, 46 (4): 81–83.

FTC. 2003. ID Theft: When Bad Things Happen to Your Good Name. http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

Freeman, Krisandra S. and Jan H. Spyridakis. 2004. An Examination of Factors That Affect the Credibility of Online Health Information. *Technical Communication*, 51 (May): 239–264.

Garbarino, Ellen and Olivia F. Lee. 2003. Dynamic Pricing in Internet Retail: Effects on Consumer Trust. *Psychology and Marketing*, 20 (June): 495–513.

Gollwitzer, Peter M. and V. Brandstatter. 1997. Implementation Intentions and Effective Goal Pursuit. *Journal of Personality and Social Psychology*, 72 (1): 186–199.

Hair, Joseph F., Ronald L. Tatham, Rolph E. Anderson, and William Black. 1998. *Multivariate Analysis*. 5th edition. Upper Saddle River, NJ: Prentice Hall.

Han, Peter and Angus Maclaurin. 2002. Do Consumers Really Care about Online Privacy? *Marketing Management*, 1 (January/February): 35–38.

Havlena, William J. and Wayne S. DeSarbo. 1991. On the Measurement of Perceived Consumer Risk. *Decision Sciences*, 22 (4): 927–939.

Henderson, Brent N., Kathryn P. Davison, James W. Pennebaker, Robert J. Gatchel, and Andrew Baum. 2002. Disease Disclosure Patterns among Breast Cancer Patients. *Psychology & Health*, 17 (February): 51–63.

Hoffman, Donna L., Thomas P. Novak, and Marcos A. Peralta. 1999. Building Consumer Trust Online. *Communications of the ACM*, 42 (April): 80–5.

Horne, Daniel R. and David A. Horne. 1997. Privacy: A Paranoid's View. In *Advances in Consumer Research*, edited by Merrie Brucks and Deborah MacInnis, vol. 14, 351–354. Provo, UT: Association for Consumer Research.

———. 1998. Domains of Privacy: Toward an Understanding of Underlying Factors. Presented at the Direct Marketing Educators' Conference, October 11. San Francisco, CA.

Horne, David A. and Daniel R. Horne. 2002. Database Marketing: When Does Good Practice Become an Invasion of Privacy? In *Marketing Theory and Applications*, edited by Kenneth Evans and Lisa Scheer, vol. 13 (480–486). Chicago: American Marketing Association.

Jacoby, Jacob and Leon B. Kaplan. 1972. The Components of Perceived Risk. In *Proceedings of the Third Annual Conference of the ACR* (382–393). Association for Consumer Research.

Jourard, Sidney M. 1971a. *Self-Disclosure, an Experimental Analysis of the Transparent Self*. New York: Wiley.

Jourard, Sidney M. 1971b. *The Transparent Self*. 2nd edition. Princeton, NJ: VanNostrand Reinhold Company.

Knapp, Linda. 2004. Identity Theft on the Rise, But It Can Be Prevented. *The Seattle Times*, January 24, 2004: C6.

Milne, George R. 1997. Consumer Participation in Mailing Lists: A Field Experiment. *Journal of Public Policy & Marketing*, 16 (Fall): 298–310.

Milne, George R. and Maria-Eugenia Boza. 1999. Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13 (Winter): 5–24.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, 38 (Winter): 217–232.

Miyazaki, Anthony D. and Sandeep Krishnamurthy. 2002. Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, 36 (Summer): 28–49.

Moon, Youngme. 2000. Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers. *Journal of Consumer Research*, 26 (March): 323–339.

Moorman, Christine, Rohit Deshpande, and Gerald Zaltman. 1993. Factors Affecting Trust in Market Research Relationships. *Journal of Marketing*, 57 (January): 81–101.

Norberg, Patricia A. 2004. Managed Profiles: The Value of Personal Information in Commercial Exchange. Unpublished Dissertation, UMI Number 3115636.

Nowak, Glen J. and Joseph Phelps. 1992. Understanding Privacy Concerns. *Journal of Direct Marketing*, 6 (Autumn): 28–39.

O'Harrow, Robert Jr. 2005. *No Place to Hide*. New York: Free Press.

O'Keefe, Daniel J. 2002. *Persuasion Theory and Research*, 2nd edition. Thousand Oaks, CA: Sage Publications.

Ouellette, Judith A. and Wendy Wood. 1998. Habit and Intention in Everyday Life: The Multiple Processes by Which Past Behavior Predicts Future Behavior. *Psychological Bulletin*, 124 (1): 54–74.

Peter, J. Paul and Lawrence X. Tarpey, Sr. 1975. A Comparative Analysis of Three Consumer Decision Strategies. *Journal of Consumer Research*, 2 (June): 29–37.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy and Marketing*, 19 (Spring): 27–41.

Potter, Jennifer E. 2002. Do Ask, Do Tell. *Annals of Internal Medicine*, 137 (5): 341–345.

Rosenberg, Alexander. 2000. Privacy as a Matter of Taste and Right. In *The Right to Privacy*, edited by E. F. Paul, F. D. Miller, and J. Paul (68–90). Cambridge, UK: Cambridge University Press.

Sayre, Shay and David A. Horne. 2000. Trading Secrets for Savings: How Concerned Are Consumers about a Privacy Threat from Club Cards? In *Advances in Consumer Research*, vol. 27 (151–155). Provo, UT: Association for Consumer Research.

Schoeman, Ferdinand D. 1984. Privacy: Philosophical Dimensions of the Literature. In *Philosophical Dimensions of Privacy*, edited by Ferdinand D. Schoeman (1–34). Cambridge, UK: Cambridge University Press.

Schoenbachler, Denise D. and Geoffrey L. Gordon. 2002. Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing. *Journal of Interactive Marketing*, 16 (Summer): 2–16.

Scholz, John T. and Mark Lubell. 1998. Trust and Taxpaying: Testing the Heuristic Approach to Collective Action. *American Journal of Political Science*, 42 (April): 398–417.

Sheehan, Kim Bartel and Mariea Grubbs Hoy. 2000. Dimensions of Privacy Concern among Online Consumers. *Journal of Public Policy and Marketing*, 19 (1): 62–73.

Sheeran, Paschal, Sheina Orbell, and David Trafimow. 1999. Does the Temporal Stability of Behavioral Intentions Moderate Intention-Behavior and Past Behavior-Future Behavior Relations? *Personality and Social Psychology Bulletin*, 25 (6): 721–730.

Skotko, Vincent P. and Daniel Langmeyer. 1977. The Effects of Interaction Distance and Gender on Self-Disclosure in the Dyad. *Sociometry*, 40 (2): 178–182.

Smith, H. Jeff, Sandra J. Millberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20 (2): 167.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences vs. Actual Behavior. In *ACM EC'01*, October 14–17, 2001.

Wasserstrom, Richard A. 1978. Privacy: Some Arguments and Assumptions. In *Philosophical Law*, edited by Richard Bronaugh. Westport, CT: Greenwood Press.

Westin, Alan F. 1996. *1996 Equifax/Harris Consumer Privacy Survey*. Atlanta, GA: Equifax.

White, Tiffany Barnett. 2004. Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology*, 14 (1 and 2): 41–51.

Whiting, Rick. 2002. Wary Customers Don't Trust Businesses to Protect Privacy. *Information Week*, August 19, 2002: 34.

Williams, Elisa. 2002. The Man Who Knows Too Much. *Forbes*, November 11, 2002: 68–70.