STRATEGIES FOR REDUCING ONLINE PRIVACY RISKS: WHY CONSUMERS READ (OR DON'T READ) ONLINE PRIVACY NOTICES

GEORGE R. MILNE AND MARY J. CULNAN

Online privacy notices are intended to promote consumer choice and reduce the risks of disclosing personal information online. However, these effects result only if consumers read and use the information contained in the notices. This study used an online survey of 2,468 U.S. adult Internet users to investigate why online consumers read privacy notices across a variety of situations. We found that reading is related to concern for privacy, positive perceptions about notice comprehension, and higher levels of trust in the notice. This suggests that effective privacy notices serve an important function in addressing risk issues related to e-commerce. We further found that reading privacy notices is only one element in an overall strategy consumers use to manage the risks of disclosing personal information online.

JOURNAL OF INTERACTIVE MARKETING VOLUME 18 / NUMBER 3 / SUMMER 2004
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/dir.20009

GEORGE R. MILNE
is associate professor of marketing at the Isenberg School of Management, University of Massachusetts, Amherst; e-mail: Milne@mktg.umass.edu

MARY J. CULNAN is the Slade Professor of management and information technology at Bentley College.

This research was partially supported by the Metromail cy pres fund. This fund was established as a result of the Dennis v. Metromail lawsuit to fund efforts related to consumer privacy.

The authors appreciate the helpful suggestions of Donna Hoffman and Shalini Bahl on earlier versions of this manuscript.

INTRODUCTION

The importance of information in consumer decision making as a way of minimizing risk has a long history in marketing. In particular, researchers have noted that information disclosure by marketers can improve consumer decision-making and choice (Beales, Craswell, & Salop, 1981; Bettman, 1975; Hadden, 1986).

The Internet as distribution channel raises issues related both to consumer risk and the effectiveness of information disclosure (Mazis & Morris, 1999). Previously, consumer marketing transactions were typically operationalized in terms of a single utilitarian exchange where goods or services are given in return for money or other goods (Bagozzi, 1975). However, due to the nature of the medium, Internet commerce also involves a "second exchange" where consumers also make a non-monetary exchange of their personal information for value such as higher quality service, personalized offers, or discounts when they visit and interact with Web sites. (Culnan & Milberg, 1998; Glazer, 1991; Milne & Gordon, 1993).

If the online environment is perceived as excessively risky, this will adversely affect the likelihood of consumers purchasing online (Hoffman, Novak, & Peralta, 1999). For e-commerce, both exchanges potentially involve a level of risk, particularly for Web sites without an established customer base, offline presence, or a strong brand (e.g., Gefen, Karahanna, & Straub, 2003; Stewart, 2003). With the first exchange, a major risk is fraud, the risk that the Web site may not deliver what it has promised. With the second exchange, online consumers face risks to their privacy when they visit Web sites (Culnan & Bies, 2003; Miyazaki & Fernandez, 2000).

Much has been written about the risk attributed to the collection of personal information without the consumers' awareness or permission (e.g., Dommeyer & Gross, 2003) and the fact that, once collected, information can easily be transferred to third parties with whom the consumer does not have an established business relationship (Caudill & Murphy, 2000; Sheehan & Hoy, 2000). Further, the online environment also makes it possible to collect new forms of personal information, such as clickstream data or location data, that go beyond traditional transaction information (Winer, 2001). In the face of these risks, disclosing information to an online organization requires a degree of trust because of information asymmetries that limit the consumer's knowledge about the organization's information practices and whether their personal information may be used in ways that could result in harm to the consumer, or lead to unwanted future solicitations, credit card theft, or even a hijacking of one's online identity.

Privacy notices are an important means for reducing the risk of the second exchange by providing consumers with information about the organization's information practices. This information can help the consumer decide whether not to disclose information to an online marketer, or whether or not to even engage with the Web site at any level (Culnan & Milberg, 1998). For database marketers in an online environment, collection of personal information as well as data pertaining to Web site visits, pages viewed, ads and products examined, the time spent on the site, and purchases made is central to executing their marketing strategy (Winer, 2001). Thus, it behooves an online marketer to create a trusted environment that will facilitate these data exchanges (Hoffman et al., 1999). Creating trust has been identified as an approach for organizations to increase information disclosures from consumers (Milne & Boza, 1999; Schoenbachler & Gordon, 2002) as well as providing the backbone of a successful online strategy (Culnan & Milberg, 1998; Sultan & Moraaj, 2001).

As described above, research has begun to examine the antecedents and consequences of reducing risks online. However, the role of online privacy notices in creating a trusted environment has not been examined. In creating a favorable environment for the second exchange, online marketers need to pay attention both to the content of the privacy notice—that privacy notices reflect whether or not the Web site observes fair information practices—and to format—that notices can be read and understood by consumers (Milne & Culnan, 2002).

Recent research found that most Web sites contained some type of privacy notice (Adkinson, Eisenach, & Lenard, 2002). While both laws and self-regulatory programs defined standards for the content some privacy notices were required to include, there were no standards for language or for the format of privacy

notices, either online and offline. As a result, privacy notices have been criticized for being of low use to consumers (Hochhauser, 2001; Schwartz, 2001). This study examines why online consumers read online privacy notices across a variety of situations based on data from an online survey of 2,468 U.S. adult Internet users.

The remainder of our paper is organized as follows. First, we develop a conceptual framework and a set of research hypotheses that guides our empirical effort. Second, we describe the survey methodology, measures, and methods used. Next, we report our results. We discuss the managerial implications of our results in a fourth section, and conclude with a discussion of limitations and avenues for future research.

CONCEPTUAL FRAMEWORK AND RESEARCH HYPOTHESES

Prior research found that people perform a simple risk-benefit calculation in deciding whether or not to disclose their personal information (Laufer & Wolfe, 1977). If consumers perceive that the benefits of disclosure exceed the risks, both current and future, they are more likely to disclose (Culnan & Armstrong, 1999; Milne, 1997; Milne & Gordon, 1993). Privacy notices then, when properly drafted and prominently posted, may provide information needed to minimize the risks of disclosure, and in so doing, provide consumers with some of the assurances they need to participate in the digital economy. We posit that the decision by a consumer to read a privacy notice is related to their trust of privacy notices. Both reading and trust are influenced by level of privacy concern, the extent to which they perceive notices to be comprehensible, whether they can rely on alternatives to notices to reduce risk, and their demographics including education, age, and online experience.

The conceptual model in Figure 1 suggests that concern for privacy, perceived notice comprehension, and demographic factors directly impact the tendency to read notices and consumers trust of privacy notices. In addition, reading a privacy notice is only one strategy a consumer might employ to manage online disclosure risks. For example, consumers may choose not to read a privacy notice if alternatives exist for managing risk (Shapiro, 1987). In the remaining part of this section, we discuss the theory for the key constructs and relationships posited in this model.

Read Privacy Notices

The extent to which consumers read notices should be influenced by context. While the literature has not examined the tendency to read notices, previous privacy studies have found that consumer willingness to disclose personal information depends on sensitivity of information (Milne, 1997; Phelps, Nowak, & Ferrell, 2000), or whether information is going to be shared with others or transferred to third parties (Milne & Boza, 1999). Further, cookies potentially

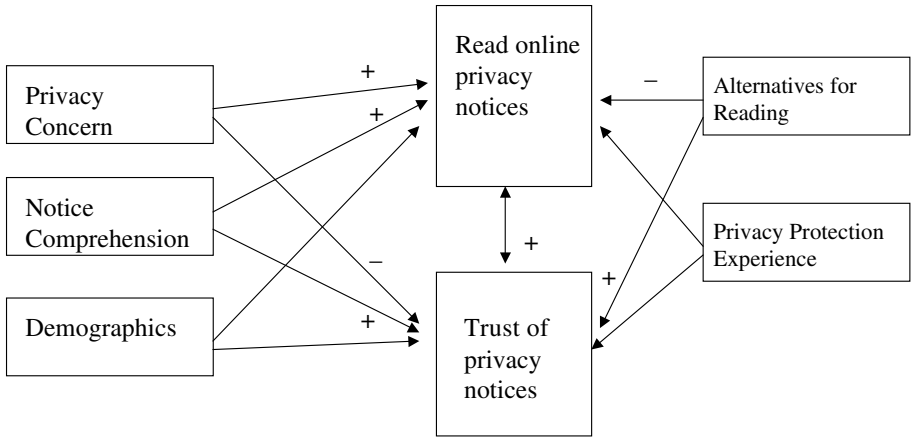

FIGURE 1
Conceptual Model

represent a surreptitious means of collecting personal information online as opposed to the consumer explicitly disclosing the information. As these variables represent potential sources of risk, they should be factors in the decision to read notices. Additional risks exist if the consumer is visiting a Web site for the first time and is therefore likely to be unfamiliar with the Web site's information practices, or if the Web site has changed its privacy policy and therefore new rules may apply to how it collects or uses personal information.

Trust of Privacy Notice

In marketing and elsewhere, trust has been conceptualized as the promise of a party to do something in the future in the interest of joint gain (Doney & Cannon, 1997). Trust has been defined as reflecting a set of specific beliefs dealing primarily with the integrity, benevolence, and ability of another party as well as the willingness of a party to be vulnerable to the actions of another (Gefen et al., 2003). Trust by definition, then, involves the willingness to assume a level of risk in the face of incomplete information. Thus, for a consumer to trust a business, they have to believe that the business will do what it says it will do and will not behave opportunistically. See Gefen et al. (2003) for a full review of the trust literature.

Trust has been identified as a key construct in the study of database marketing (Milne & Boza, 1999; Schoenbachler & Gordon, 2002) and online marketing (Hoffman et al., 1999). Milne and Boza (1999) and Culnan and Milberg (1998) both argue that for privacy notices to build trust, the message should be informative and reassure consumers that disclosing their personal information is a low-risk proposition. Schonenbachler and Gordon (2002) note that having a clear and credible privacy notice helps marketers build a positive reputation with consumers.

Due to the risks involved in doing business online, consumers have incentives to read privacy notices to learn about the organization's stated policies prior to engaging in transactions. If consumers find these notices useful, this may lead them to trusting the notices more. However, consumers may not invest the time and effort to read the notices if they do not trust the Web site to comply with its notice or if they do not believe the notice itself is an accurate reflection of the organization's information practices. Further, use of nutritional labels has been shown to be related to trust in labels (Balasubramanian & Cole, 2002). Because of this reasoning, we expect the level of trust of notices to be related to whether one reads a privacy notice or not.

H1: Trust of online privacy notices is positively associated with a tendency to read online privacy notices.

Privacy Concern

Consumers seek information to reduce risk the risk of consuming a particular product or service where risk reflects perceptions of the uncertainty and the adverse consequences of consuming a product or service (Dowling & Staelin, 1994; Ingene & Hughes, 1985). Comparative advertising research has shown that consumers pay close attention to marketing communications that are personally relevant (Pechmann & Stewart, 1990). In the labeling and warnings literature, concern about health issues has been positively related to consumers' tendencies to read labels and process warning messages (Szykman, Bloom, & Levy, 1997). We expect that this relationship between concern and reading should also hold true for online privacy notices.

Privacy is defined in terms of individual control over disclosure and subsequent uses of their personal information (Westin, 1967); the greater the perceived control, the less the risk. Public opinion surveys continue to find that a majority of consumers express concern about losing control over the ways in which organizations handle their personal information (Harris Interactive, 2002). For example, one survey found that for people who had provided false information to a Web site or declined to provide information, 63% said they would have supplied the information if the site provided notice about how the information would be used prior to disclosure, and the consumer was comfortable with these uses (Harris Interactive & Westin, 1997). However, the relationship between concern and motivation to read the notice has not been tested empirically. Therefore, as privacy notices provide information to assess the risks of disclosing personal information, we expect

people with higher concern for privacy will be more likely to read online privacy notices than people who are less concerned.

H2a: Concern for privacy is positively associated with a tendency to read online privacy notices.

Concern for privacy should also be related to the extent to which consumers trust online privacy notices (Schoenbachler & Gordon, 2002). For example, Milne and Boza (1999) found that concern was negatively related to trusting organizations to use personal information fairly, suggesting that this relationship should transfer to the privacy notices that describe the organization's information practices.

H2b: Concern for privacy is negatively associated with trust of online privacy notices.

Perceived Comprehension

Research in the label and warning area has shown that the content and format of labels and warnings are directly related to the ability of consumers to process and subsequently use the information in the notice (Moorman, 1990, 1996; Stewart & Martin, 1994). In particular, the human factors literature suggests factors such as readability, noticeability, framing effects, and explicitness of conclusions all impact information processing of warnings (Lethto & Miller, 1986; Wogalter et al., 1987). Previous research on the readability of warnings found that consumers may not comprehend the words often used in warning messages (Pyrczak & Roth, 1976). These findings should extend to privacy notices since privacy notices serve a function that is roughly analogous to a warning. We expect consumers will be more likely to read privacy notices when they perceive they are presented in a format they can comprehend and subsequently use.

H3a: Perceived comprehension of privacy notice is positively associated with a tendency to read online privacy notices.

Further, Balasubramanian and Cole (2002) found that, for nutritional labels, claims that were hard to verify or were disclosed in ways that were not meaningful to consumers were related to greater skepticism in the notice. Alternatively, privacy notices with a straightforward exposition should engender trust (Gefen et al., 2003).

H3b: Perceived comprehension of privacy notices is positively associated with trust of online privacy notices.

Alternatives for Reading Notices

Reading privacy notices is but one way consumers can learn about an organization's information practices. Consumers may rely on alternative signals that provide assurances their information is safe such as a privacy seal or the reputation or brand of the company (Gefen et al., 2003; Shapiro, 1987). Further, consumers may not read the privacy notice if they have prior online or offline experience with the firm. For product warnings, consumers with prior product experience were less likely to read notices (Stewart & Martin, 1994). This suggests:

H4a: Use of alternatives for reading notices will be negatively associated with reading privacy notices.

However, prior experience has also been shown to be positively related to online trust (Gefen et al., 2003). This suggests:

H4b: Use of alternatives for reading notices will be positively related to trust of notices.

Demographic Factors

Previous research on labeling has examined the impact of customer demographic characteristics on information utilization (Moorman, 1990; Cole & Gaeth, 1991; Stewart & Martin, 1994). For example, age and education should affect an individual's ability to read and understand privacy notices. Moorman (1990) found a significant positive relationship between education and a positive but non-significant relationship between age and motivation to use nutritional information. Prior research on privacy found gender, age, education, and experience online to be associated with privacy concerns or with trust (Dommeyer & Gross, 2003; Schoenbachler & Gordon, 2002). Therefore, we expect to find that demographic differences are associated with reading or not reading privacy notices. Finally, prior research found involvement to be a key predictor of consumer information processing (Moorman 1990). We also include a behavioral measure of involvement, steps taken by the individual to protect their privacy online, and expect

engaging in privacy protection to be positively associated with reading notices.

METHOD

Survey Development and Sample

The research was conducted as a field study. The questionnaire was pretested using a Web-based survey program. Faculty, staff and students at the authors' respective institutions were sent an e-mail inviting them to participate in the survey. A clickable URL was provided in the e-mail that directed them to the survey form. The pretest resulted in 122 useable responses. The reliabilities for the research constructs were all within acceptable ranges.

Harris Interactive administered the final survey and collected data online from November 6–8, 2001. A stratified random sample of 2,468 U.S. adults was drawn from the multi-million member Harris Poll Online panel based upon known proportions of age, gender, and region in the U.S. population. The demographics of the sample are shown in Table 1. Appendix A describes the sampling methodology used by Harris Interactive.

Measurement

Survey respondents were asked how frequently they read privacy notices posted by Web sites using a five-point scale ranging from 1 = never read them to 5 = always read them. We used this item to divide our respondents into two categories: readers (83.7%) and non-readers (17.3%). In testing our hypotheses, we excluded non-readers because logically they could not respond to questions about why they read privacy notices, perceived comprehension, or trust of notices. For the readers, 4.5% indicated they always read, 14.1% indicated they frequently read, 31.8% indicated

TABLE 1 Demographics of the Sample

(***N*** **= 2468)**

PARAMETER	%	PARAMETER	%
Gender		Income	
Males	51.9	Less than $49,999	39.5
Females	48.1	$55, 000 to $99,999	30.1
		$100,000 and over	11.4
Age		Declined to answer	18.9
18–34	31.9		
35–54	39.4	Ethnicity	
55 and over	28.6	White	87.1
		Other than white	6.7
Marital Status		Decline to answer	6.1
Married	56.3		
Not married	39.7		
		Employment Status	
Education		Employed full-time	53.8
Less than high school	0.6	Employed part-time	7.0
Completed some high school	1.7	Self-employed	6.0
High school graduate or equivalent	12.3	Not employed, but looking for work	3.7
Completed some college, but no degree	40.1	Not employed, not looking for work	2.1
College graduate	24.1	Retired	14.1
Completed some graduate school, but not degree	7.3	Student	7.8
		Homemaker	5.5

they sometimes read, and 33.3% indicated they rarely read online privacy notices.

The survey also included two open-ended questions. Subjects who responded that they never read privacy notices were asked "Why have you chosen not to read privacy notices posted by Web sites?" Subjects who indicated that they read privacy notices at least rarely were also asked to provide other reasons they might have for reading or not reading a Web site's privacy notice in addition to the reasons posed in the survey. The content of these responses was not formally analyzed, however we grouped the responses into categories to provide additional richness to our quantitative results.

Dependent Variables

Reasons for Reading Notices. The first dependent variable, reasons for reading notices, was measured using seven five-point scaled items (1 = strongly disagree to 5 = strongly agree) reflecting situations where a consumer might read a privacy notice. The items measured situations where the consumer would read the privacy notice (e.g., "I usually read the privacy notice if I am visiting a Web site for the first time"). We created a scale, "reasons for reading," by averaging the values from the seven items. The coefficient alpha for this scale was 0.86. Details on the items for all multi-item scales are shown in Appendix B.

Trust of Privacy Notices. Trust of privacy notices was measured using five five-point items (1 = strongly disagree to 5 = strongly agree) adapted from Moorman's (1996) skepticism in food label information scale. A representative item was "Web privacy notices accurately reflect how Web sites use the information they collect from me." The coefficient alpha was 0.82.

Independent Variables

Concern for Privacy. Concern for privacy was measured using five five-point scaled items (1 = strongly disagree to 5 = strongly agree). The scale was adapted from the "Information Privacy Concern scale" developed by Smith, Milberg, and Burke (1996). A representative item was "I'm concerned that companies are collecting too much personal information from me." The coefficient alpha was 0.88.

Perceived Comprehension of Privacy Notices. Perceived comprehension of privacy notices was measured using five five-point scaled items (1 = strongly disagree to 5 = strongly agree). A representative item was "Web privacy notices are usually easy to understand." The coefficient alpha was 0.77.

Alternatives for Reading Notices. Alternatives for reading privacy notices was measured using three items: (1) prior experience with the company, (2) whether Web site belongs to a well-known company, and (3) whether the Web site displays a privacy seal. These items used five-point scales "I usually do not read the privacy notice if . . ." ranging from 1 = strongly disagree to 5 = strongly agree. We averaged the item values to create a scale, "substitutes for reading." The coefficient alpha was 0.73

Demographic Variables

Demographic variables of age, education, experience (hours online per week) and gender were based on the standard demographic measures provided by Harris Interactive. Age was measured by 11 categories ranging from "18–19" to "65 and over." Education was measured by seven categories ranging from "Less than high school" to "Completed graduate school." The median value of each category was used to convert age to year old and education to years of schooling. Hours online was measured first as the number of hours a week spent on the Internet or World Wide Web, excluding e-mail. Table 2 contains differences between readers and non-readers for the demographic variables. There were statistically significant differences noted between the readers and non-readers of privacy notices in terms of overall privacy concern and age (readers were more concerned and older). However, no differences were found for level of education or hours online.

Privacy protection experience was measured using a formative scale based on whether the subject had performed the following six activities: "Refused to give information to a Web site because you felt it was too personal or unnecessary" (84.8%); "Asked a Web site to remove your name and address from any lists used for marketing purposes" (82.8%); "Asked a Web site not to share your name or other personal information with other companies" (79.4%); "Decided not to use a Web site or not purchase something from a Web site

TABLE 2 Comparison of Non-Readers and Readers of Online Privacy Notices

PARAMETER	NON-READERS	READERS	T VALUE	PROBABILITY
N	402	2066		
Concern for Privacy	19.1	19.7	−3.42	0.001
Age	44.9	49.7	−6.89	0.000
Education	14.7	14.7	0.13	0.897
Experience (Hours Online)	15.3	15.0	0.52	0.605
Privacy Protection Experience	3.5	3.8	−4.53	0.000
PRIVACY PROTECTION EXPERIENCE BREAKDOWN	**NON-READERS**	**READERS**	**CHI-SQUARE**	**PROBABILITY**
Refused to give information to a Web site because it was too personal or unnecessary	72.6%	87.2%	55.68	0.000
Asked a Web site to remove your name and address from any lists used for marketing purposes	78.1%	83.7%	7.35	0.007
Asked a Web site not to share your name or other personal information with other companies	72.1%	80.8%	15.36	0.000
Decided not to use a Web site or not purchase something from a website because you were not sure of how your personal information would be used	51.7%	66.3%	30.76	0.000
Set your computer browser to reject cookies	30.8%	32.0%	0.25	0.651
Supplied false or fictitious information to a Web site when asked to register	42.5%	32.4%	15.46	0.000

because you were not sure how your personal information would be used" (63.9%); "Set your computer or browser to reject cookies" (31.8%); "Supplied false or fictitious information to a Web site when asked to register" (34.0%). Table 2 also contains differences between readers and non-readers for privacy protection experience. With the exception of rejecting cookies, readers are significantly more likely to engage in these behaviors than non-readers.

The survey items measuring the variables reasons for reading, trust of privacy notices, privacy concern, perceived comprehension, and alternatives for reading were analyzed using a principal components factor analysis to assess the dimensionality of the constructs. The resulting five-factor solution based on eigenvalues greater than 1, explained 62.3% of the variance and revealed that all the items loaded cleanly on their intended factors (See Appendix B).

RESULTS

We tested our hypotheses with multivariate regressions. The "reasons for reading" and "trust of notice" scales, which were positively correlated ($r = 0.062$, $p < 0.01$), respectively served as the dependent variables. The regressions explaining reasons for reading (adjusted $R^2 = 0.244$, $F = 65.10$, $p < 0.01$) and trust in notices (adjusted $R^2 = 0.158$, $F = 38.22$, $p < 0.01$) were both statistically significant. Table 3 contains the multivariate tests for the general linear model and the coefficients for the two separate regressions.

The significant positive correlation between the dependent variables, read online privacy notices and trust privacy notices, supports H1. In examining the coefficients across the models, concern for privacy is positively related to reasons for reading ($\beta = 0.261$; $p < 0.01$), supporting H2a, and negatively related to

TABLE 3 Multivariate Regression Results for Reading Notices and Trust of Notices

PARAMETER	WILK'S λ	PROB. OF F	REASONS FOR READING	TRUST OF NOTICE
Concern for Privacy	0.925	0.000	**0.261**	**−0.213**
Comprehension of Notice	0.934	0.000	**0.186**	**0.217**
Alternatives for Reading	0.872	0.000	**−0.712**	**0.073**
Privacy Protection Experience	0.978	0.000	**0.575**	−0.058
Education	0.997	0.114	**−0.122**	−0.035
Age	0.973	0.000	**0.055**	**−0.022**
Sex (Male=1)	0.981	0.000	**−0.896**	**−0.697**
Hours on the Web	0.992	0.002	0.016	**−0.017**
Overall Significance (*F*)			65.10 ($p < 0.01$)	38.22 ($p < 0.01$)
Adj. R^2			0.244	0.158

Note. Coefficients in bold are significant at the 0.05 level.

trust of notice ($\beta = -0.213$; $p < 0.01$), supporting H2b.

For the coefficient perceived comprehension of notice, both hypothesized relationships for reading and trust of notice (H3a,b) were supported by the data. Specifically, perceived comprehension of notice was found to be positively related to reasons for reading ($\beta = 0.186$, $p < 0.01$), and positively related to trust of notice ($\beta = 0.217$; $p < 0.01$).

The Open-Ended Responses Support These Results. In their comments, respondents complained that notices were too long or boring. "Privacy notices are deliberately made too long and verbose. How about the 'Privacy Notice for Dummies' version?'" Others complained that the format of the notice, such as the type size, made it hard to read. Still others complained about the legalist nature of the notices: "Get real, no one in their right mind WANTS to read that mumbo jumbo verbiage." ". . . I wish they would just simplify the basic points and have a long wordy version as an option and to cover their bums in case of some stupid money grubber suing them." "I don't have a law degree." Another related complaint about the notices was that they were all the same. "Because they tend to be the same boilerplate over and over again, if you read one, you've read them all." Finally despite industry efforts, some respondents were not aware of the existence of notices.

For the coefficient "alternatives for reading," H4a was supported. There was a significant negative relationship between use of alternatives and reasons for reading ($\beta = -0.712$, $p < 0.01$). These results were supported by the comments as respondents cited experience, reputation, and branding of the company as reasons people for not reading notices. However, there was a positive relationship between the use of alternatives and trust of notices, supporting H4b ($\beta = 0.073$, $p < 0.01$).

Respondents who had prior experience with a company, and had no reason to believe the Web site had changed its practices since their last visit indicated that the risk of dealing with the site was acceptable and there was no reason to read the notice. For example, comments included, "I only buy from trusted Web sites—stores I've already experienced offline, so just assume I'm protected." "I only give personal information to companies or organizations I know. I have a few sites I purchase from. If a site starts asking questions, I leave." "I generally do Internet business with the same companies and have grown to trust them. So far, those companies have not betrayed me." Respondents also cited making a first visit to a firm's

Web site as a reason for reading notices. "I don't read them if it is a site I use often. I do read them when using a site for the first time."

For the demographic variables, age is positively related to reading ($\beta = 0.055$, $p < 0.01$), and negatively related to trust ($\beta = -0.022$, $p < 0.01$). The results for education were negatively related to both reading ($\beta = -0.122$, $p < 0.05$) but not significantly to trust ($\beta = -0.035$, $p > 0.05$). Males were less likely to read notices ($\beta = -0.896$, $p < 0.01$) and to trust Web-site notices ($\beta = -0.697$, $p < 0.01$). Experience measured as hours on the Web was not related to reasons for reading notices ($\beta = 0.016$, $p > 0.05$) and was negatively related to trust of notices ($\beta = -0.017$, $p < 0.05$). Finally, there was a significant positive relationship ($\beta = 0.575$, $p < 0.01$) between privacy protection experience and reasons for reading, and a non-significant relationship for trust ($\beta = -0.058$, $p > 0.05$).

DISCUSSION

This study examined reasons and situations when consumers read privacy notices and where they use alternatives for privacy notices. The results suggest that privacy notices are used as one part of an overall strategy to manage the risks of disclosing personal information and that consumers tend to read notices to manage risk. The finding that consumers tend not to read privacy notices when they have prior experience with a firm suggests that privacy notices should prove to be the most important for sites that do not have a strong brand or are new.

For the respondents who read privacy notices, control over personal information emerged in the open-ended comments as a main reason for reading the notices, especially when consumers were asked to disclose sensitive information. "I always read the privacy notice for any credit card company or an application for a credit card." Others read notices to see how their personal information would be used, particularly if it would be shared with other organizations, for example, "I tend to read just the portion that indicates they don't 'share' my information." Much of this appeared to stem from concerns over receiving unwanted e-mail. For example, one respondent stated they will read notices "if I start getting a lot of junk postal mail or e-mail for no apparent reason."

Still others felt that there was no risk-based reason to read notices. "I am sure that the sites are doing everything to protect me and my privacy." "Never had any problems with the way my information is used. I trust that the appropriate authorities are regulating how my information is used." Some respondents reported that the act of posting a notice minimized the risks of doing business with the Web site: ". . . I find that if they are willing to post their privacy notice, they are reputable enough to keep my information confidential." This is consistent with the results of a more recent survey that found that the act of posting a privacy notice provided unwarranted assurances to consumers about the Web site's actual practices (Turow, 2003).

While privacy concern remains a big motivator for consumers to read notices, the study also found that perceived comprehension of notices also had a strong effect. If the notice is not perceived as comprehensible, then it will be less likely to be read. Many of the qualitative comments echo this finding and reflected frustration about the lengthy and legalistic documents these notices have become. Alternatively, when consumers perceive they can comprehend privacy notices, the more likely they are to both read notices across an array of situations and to trust the notices. Further, some of the comments also suggested that notices that are perceived by consumers to be obfuscated or excessively legalistic can contribute to skepticism (Morman, 1996; Balasubramanian & Cole, 2002).

Two factors potentially affect the perceived comprehensibility of online privacy notices. First, like product labels and warnings, online privacy notices may be used for compliances purposes (Stewart & Martin, 1994). As a result, organizations write privacy notices to be exhaustive and not necessarily to be accessible to consumers and informative. The likelihood of this is increased since the conditions and terms relating to future use of the information consumers disclose may be open ended and complex. Further, a notice that does not fully disclose the firm's information practice may be the basis for an unfair or deceptive trade practice enforcement action by the Federal Trade Commission.

Second, online privacy notices are documents that can be presented in a hyper-text format. As a result, there are opportunities to promote better comprehension of online notices through the use of links than in the

offline world. The open-ended comments and other evidence such as Hochhauser (2001) suggest that many current online privacy notices do not exploit these opportunities. If consumers perceive privacy notices as being irrelevant because of format issues, they may balk at even attempting to read them as some of the open ended comments illustrate (Stewart & Martin, 1994).

One limitation of the study is that the Harris online sample may skew upwards in terms of affluence and sophistication in online actions. Clearly, only individuals who are comfortable disclosing personal information online are going to belong to such a panel and take the time to fill out a survey online. Further, this study looks only at consumers' self-reported motivations for reading online privacy notices. The study's survey methodology precluded the investigation into other motivational or behavioral aspects that have been used in the labeling and warnings literature. Future research that utilizes different research approaches, such as controlled experimentation, is encouraged in order to understand the roles privacy notices play in consumer decision-making, including the role the site's information practices policy play in the consumer's ultimate decision to begin or continue a relationship with the Web site.

The results of our study also indicate that current privacy notices need to undergo a major reform. A second survey conducted at the same time as ours measured attitudes toward both online notices and the privacy notices financial institutions were required to mail to their customers beginning in July 2001 (Harris Interactive, 2001). This survey found similar results for frequency of reading. In addition, the respondents also reported a strong preference for short privacy policies (77%) and for companies to adopt a consistent summary or checklist for their privacy policies (70%). If privacy notices are to take on the importance and usefulness of a nutritional label, a simplified, unified format that presents information in a condensed and accessible format is needed (Bettman, Payne, & Staelin, 1986; Derby & Levy, 2001).

One message of this and other research is that improving current privacy notices is an effort worth pursuing. Our findings indicate that the literature on warnings and labels provides an appropriate starting point. The challenge inherent in developing standard ways to describe information practices that vary with different business models suggest an interesting and challenging agenda for marketing researchers interested in consumer information processing and interactive marketing.

REFERENCES

Adkinson, W.F., Eisenach, J.A., & Lenard, T.M. (2002). Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites. Washington: Progress & Freedom Foundation. Retrieved June 29, 2003, from http://www.pff.org/publications/privacyonline finalael.pdf

Bagozzi, R.P. (1975). Marketing as Exchange. Journal of Marketing, 39(October), 32–39.

Balasubramanian, S.K., & Cole, C. (2002). Consumers' Search and Use of Nutrition Information: The Challenges and Promise of the Nutrition Labeling and Education Act. Journal of Marketing, 66(3), 112–127.

Beales, H., Craswell, R., & Salop, S.C. (1981). The Efficient Regulation of Consumer Information. Journal of Law & Economics, 24(December), 491–539.

Bettman, J.R. (1975). Issues in Designing Consumer Information Environments. Journal of Consumer Research, 2(December), 169–177.

Bettman, J.R., Payne, J.W., & Staelin, R. (1986). Cognitive Considerations in Designing Effective Labels for Presenting Risk Information. Journal of Public Policy and Marketing, 5, 1–28.

Caudill, E.M., & Murphy, P.E. (2000). Consumer Online Privacy: Legal and Ethical Issues. Journal of Public Policy and Marketing, 19(1), 7–19.

Cole, C.A., & Gaeth, G.J. (1990). Cognitive and Age-related Differences in the Ability to Use Nutritional Information in a Complex Environment. Journal of Marketing Research, 37(May), 175–184.

Culnan, M.J., & Armstrong, P.K. (1999). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. Organization Science, 10(January), 104–115.

Culnan, M.J., & Bies, R.J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, 59(2), 323–342.

Culnan, M.J., & Milberg, S.J. (1998). The Second Exchange: Managing Customer Information in Marketing Relationships. Georgetown University, Unpublished Working Paper.

Derby, B.M., & Levy, A.S. (2001). Do Food Labels Work? Gauging the Effectiveness of Food Labels Pre- and Post-NLEA. In P. Bloom & G.T. Gundlach (Eds.), Handbook of

Marketing and Society (pp. 372–398). Thousand Oaks: Sage Publications, Inc.

Doney, P., & Cannon, J.P. (1997). An Examination of the Nature of Trust in Buyer-Seller Relationships. Journal of Marketing, 61(2), 35–61.

Dommeyer, C.J., & Gross, B. (2003). Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. Journal of Interactive Marketing, 17(2), 34–51.

Dowling, G.R., & Staelin, R. (1994). A Model of Perceived Risk and Intended Risk-Handling Activity. Journal of Consumer Research, 21(June), 119–134.

Gefen, D., Karahanna, E., & Straub, D.W. (2003). Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly, 27(1), 51–90.

Glazer, R. (1991). Marketing in an Information-Intensive Environment: Strategic Implications of Knowledge as an Asset. Journal of Marketing, 55(October), 1–19.

Hadden, S.G. (1986). Read the Label: Reducing Risk by Providing Information. Boulder, CO: Westview Press.

Harris Interactive, Inc. (2001). Privacy Notices Research: Final Results. Retrieved October 21, 2002, from http://www.ftc.gov/bcp/workshops/glb/index.htm

Harris Interactive, Inc. (2002). Privacy On and Off the Internet: What Consumers Want. Hackensack: Privacy and American Business.

Harris Interactive, Inc., & Westin, A.F. (1997). Commerce, Communication and Privacy Online. Hackensack: Privacy and American Business.

Hochhauser, M. (2001). Lost in the Fine Print: Readability of Financial Privacy Notices, San Diego: Privacy Rights Clearinghouse. Retrieved from http://www.privacyrights.org

Hoffman, D.L., Novak, T.P., & Peralta, M. (1999). Building Consumer Trust Online. Communications of the ACM, 42(4), 80–85.

Ingene, C.A., & Hughes, M.A. (1985). Risk Management by Consumers. In. J.N. Sheth (Ed.), Research in Consumer Behavior, (Vol. 1, pp. 103–158). Greenwich, CT: JAI Press, Inc.

Laufer, R.S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues, 33, 22–42.

Lehto, M.R., & Miller, J.M. (1986). Warnings: Fundamentals, Designs, and Evaluation Methodologies. Ann Arbor, MI: Fuller Technical Publications.

Mazis, M.B., & Morris, L.A. (1999). Channel. In M.S. Wogalter, D.M. Dejoy, & K.R. Laughery (Eds.), Warnings and Risk Communication (pp. 99–121). Philadelphia: Taylor & Francis, Inc.

Milne, G.R. (1997). Consumer Participation in Mailing Lists: A Field Experiment. Journal of Public Policy and Marketing, 16, 298–309.

Milne, G.R., & Boza, M. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. Journal of Interactive Marketing, 13(1), 5–24.

Milne, G.R., & 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, 18(5), 345–360.

Milne, G.R., & Gordon, M.E. (1993). Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework. Journal of Public Policy and Marketing, 12(Fall), 206–215.

Miyazaki, A., & Ferdnandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. Journal of Public Policy and Marketing, 19(1), 54–61.

Moorman, C. (1990). The Effects of Stimulus and Consumer Characteristics on the Utilization of Nutrition Information. Journal of Consumer Research, 17(3), 362–374.

Moorman, C. (1996). A Quasi Experiment to Assess the Consumer and Informational Determinants of Nutrition Information Processing Activities: The Case of the Nutrition Labeling and Education Act. Journal of Public Policy and Marketing, 15(1), 28–44.

Pechman, C., & Stewart, D.W. (1990). The Role of Comparative Advertising: Documenting Its Effects of Attention, Recall, and Purchase Intentions. Journal of Consumer Behavior, 17(September), 2.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy and Marketing, 19(1), 27–41.

Pyrczak, F., & Roth, D.H. (1976). The Readability of Directions on Non-Prescription Drugs. Journal of the American Pharmaceutical Association, 16(May), 242–243, 267.

Schoenbachler, D.D., & Gordon, G.L. (2002). Trust and Consumer Willingness to Provide Information in Database-Driven Relationship Marketing. Journal of Interactive Marketing, 16(3), 2–16.

Schwartz, J. (2001). Privacy Policy Notices Are Called too Common and too Confusing. New York Times, May 7.

Shapiro, S.P. (1987). The Social Control of Impersonal Trust. American Journal of Sociology, 93(3), 623–658.

Sheehan, K.B.,& Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy and Marketing, 19(1), 62–73.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information Privacy: Measuring Individual's Concerns About Organizational Practices. MIS Quarterly, 20(2), 167–196.

Stewart, D.W., & Martin, I.M. (1994). Intended and Unintended Consequences of Warning Messages: A Review and Synthesis of Empirical Research. Journal of Public Policy and Marketing, 13(1), 1–19.

Stewart, K.J. (2003). Trust Transfer on the World Wide Web. Organization Science, 14(1), 5–18.

Sultan, F., & Mooraj, H.A. (2001). Designing a Trust-Based e-Business Strategy. Marketing Management, 10(4), 40–46.

Szykman, L.R., Bloom, P.N., & Levy, A.S. (1997). A Proposed Model of the Use of Package Claims and Nutritional Labels. Journal of Public Policy and Marketing, 16(2), 228–241.

Turow, J. (2003). Americans and Online Privacy: The System is Broken. Annenberg Public Policy Center, University of Pennsylvania, June. Retrieved June 25, 2003, from http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf

Westin, A. (1967). Privacy and Freedom. New York: Athenaeum.

Winer, R.B. (2001). A Framework for Customer Relationship Management. California Management Review, 43(4), 89–108.

Wogalter, M.S., Godfrey, S.S., Fontenelle, G.A., Desaulniers, D.R., Rothstein, P.R., & Laughery, K.R. (1987). Effectiveness of Warnings. Human Factors, 29(5), 599–612.

APPENDIX A SAMPLING METHODOLOGY

The survey was conducted as a Harris Interactive Quick Query. Harris Interactive draws subjects from its multi-million member Harris Poll Online (HPOL) panel so that the characteristics of those invited to participate are descriptively representative of the U.S. general adult population. Here, a stratified random sample was drawn from the HPOL members based upon their known proportions by age, gender, and region in the U.S. population. Harris then adjusts gender proportions to account for the differential response rates of men and women as women tend to respond at slightly higher rates.

Survey invitations were initially e-mailed to 34,903 panel members. One day later, an additional 5,271 invitations were e-mailed to females aged 30 or older for a total of 40,168 invitations. Reminders were mailed one day later to 33,257 individuals in the first group who had not yet responded. The survey was in the field for 41 hours.

Of the initial pool, 2,499 individuals completed the survey. An additional 267 individuals began the survey but did not complete it. Of people who began the survey, the within-survey completion rate was 90.3%. The overall response rate was 6.9%.

Unlike telephone and mail surveys, where invalid addresses, telephone numbers, and refusals can be measured, there is no way of knowing how many people actually saw the initial survey invitations but declined to answer. As a result, Internet survey response rates routinely appear to be lower than response rates for other survey methods. In general, HPOL response rates vary from 5–50% depending on the survey invitation subject line, the incentive offered, survey length and topic, ease of use of the survey itself, etc.

Harris argues unequivocally that low response rates do not mean the results are not representative, due to the two-stage approach taken to balancing the sample. In the first stage, the responses are balanced by gender. Here, this meant sampling from additional females age 30 and older. In the second stage, the data are weighed by a variety of factors including age, gender, education, income, race, and region of the country. At least one academic study has found that properly weighted data collected by Harris Interactive exhibits the same behaviors as data collected properly by telephone.

APPENDIX B DESCRIPTIVE STATISTICS AND ROTATED FACTOR STRUCTURE OF SCALED VARIABLES

	Mean	*Standard Deviation*	*Reasons for Reading*	*Trust of Privacy Notices*	*Privacy Concern*	*Perceived Comprehension*	*Alternatives for Reading*
Reasons for Reading							
I usually read the privacy notice if I am using my credit card to buy something from the Web site	4.12	1.01	0.712				
I usually read the privacy notice when the Web site asks me for personal information	3.92	0.99	0.772				
I usually read the privacy notice to learn if the Web site shares my personal information with other companies	3.78	1.03	0.775				
I usually read the privacy notice to learn how the Web site will use the information it collects from me	3.57	1.02	0.802				
I usually read the privacy notice if I am visiting a Web site for the first time	3.40	1.05	0.773				
I usually read the privacy notice if I believe the Web site has changed its privacy policy	3.36	1.00	0.698				
I usually read the privacy notice to learn if the Web site uses cookies	2.77	1.04	0.593				
Trust in Notice							
Web privacy notices accurately reflect how Web sites use the information they collect from me	3.04	0.76		0.755			
Companies will follow through on statements in the Web privacy notices	3.14	0.73		0.853			
The promises companies make in their Web privacy notices are not to be trusted (R)	3.20	0.79		0.768			
I believe that Web privacy notices are truthful	3.18	0.78		0.864			
I trust companies to fulfill the promises they make in their Web privacy notices	3.39	0.93		0.782			

(*Continued*)

	Mean	*Standard Deviation*	*Reasons for Reading*	*Trust of Privacy Notices*	*Privacy Concern*	*Perceived Comprehension*	*Alternatives for Reading*
Concern for Privacy							
It usually bothers me when companies ask me for personal information	3.84	0.85			0.834		
I am concerned that companies are collecting too much personal information about me	3.96	0.84			0.818		
It bothers me to give personal information to so many companies	4.02	0.81			0.865		
When companies ask for personal information, I sometimes think twice	4.22	0.68			0.746		
Consumers have lost all control over how companies collect and use their personal information	3.67	0.97			0.570		
Perceived Comprehension							
Web privacy practices are easy to understand	2.65	0.96				0.808	
Web notices often contain terms that are confusing to me (R)	2.78	0.99				0.784	
Web privacy notices are usually organized so they are easy to follow	2.59	0.88				0.690	
Web privacy notices are often too long be useful (R)	2.18	0.92				0.553	
Web privacy notices often do not use legal language that is hard to understand or is confusing	2.50	0.98				0.842	
Alternatives for Reading							
If I have experience with a company, I usually do not read their Web site privacy notice	3.35	1.01					0.803
I usually do not read the privacy notice if the Web site belongs to a well-known company	3.23	1.07					0.773
If the Web site displays a privacy seal, I usually do not read the privacy notice	3.10	0.98					0.724
Percent of Variance Explained			19.7	19.6	9.7	7.5	5.7

Note. Principal Components Extraction, Varimax Rotation.