ROBERT LAROSE AND NORA J. RIFON

Promoting *i*-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior

Using social cognitive theory, this study experimentally examines the effects of explicit privacy warnings, a clear, conspicuous, and concise presentation of the benefits and risks associated with database information practices stated in a Web site's privacy policy. Warnings increased perceptions of the risks associated with information practices and decreased disclosures, but not in the presence of a privacy seal. The effects were also moderated by consumer privacy self-efficacy and involvement with privacy. The results support the development of privacy warnings as a part of consumer privacy self-regulatory efforts and the use of a social cognitive paradigm for understanding consumer privacy behaviors.

THE *I*-SAFETY PROBLEM

How can we motivate Internet consumers to engage in behavior that will protect their privacy online? This question assumes increasing importance as privacy threats reach alarming proportions. In a recent multicity audit of consumers' computers conducted by the National Cyber Security Alliance, four-fifths were infested with spyware (National Cyber Security Alliance 2004). One-eighth of all identity thefts are attributed to online sources including spyware, online transactions, viruses, and phishing (Better Business Bureau 2005). Two-thirds of all e-mail worldwide is now spam (MessageLabs 2005), up from 7% in 2001 (Brightmail 2004). Consumers, as well as Web site proprietors, software developers, and policy makers, must play a role in protecting privacy (Milne and Culnan 2004). However, consumers are called upon (Consumer Reports 2004; PC Magazine 2004) to enact a bewildering array of measures to protect their privacy online: update virus protection, mind security settings, download patches, install firewalls, screen e-mail, shut down spyware, control cookies, deploy encryption, fend off browser hijackers, and block pop-ups. How can the

Robert LaRose is a Professor in the Department of Telecommunication, Media and Information Studies, Michigan State University, East Lansing, MI (larose@msu.edu). Nora J. Rifon is a Professor in the Department of Advertising, Michigan State University, East Lansing, MI (rifon@msu.edu).

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

average consumer be enlisted in the abstract and complex cause of privacy protection and ultimately, network security?

Presently, Internet privacy standards have been set forth by the Federal Trade Commission (FTC), relying on the voluntary participation of Web proprietors for the provision of their information practices in a clear and conspicuous privacy policy and the participation in privacy seal programs such as TRUSTe. Yet, consumers do not appear to completely understand what seals assure (Rifon, LaRose, and Choi 2005) and most do not read policies (Turow 2003). We suggest that privacy policies and seals do not provide adequate information for consumers to understand the implications of the sharing of their personal information, nor do they motivate consumers to take protective actions and engage in safe online behaviors. A different model for notice is needed, one that can prompt consumers to consider the potential consequences, positive and negative, that are associated with personal information disclosures.

From the consumer's perspective, privacy and security measures entail managing the release of personal information while deflecting unwanted intrusions, parallel to two underlying dimensions of consumer privacy (cf. Goodwin 1991; Lee and LaRose 1994). Online privacy may then be defined in behavioral terms as actions that prevent unwanted disclosures and intrusions while using the Internet. As such, consumers translate preferences into actions that protect themselves, their information, and their computers. We conceptualize the problem as one of personal safety protection, arming consumers with the requisite information and skills so that they can make informed choices and enact appropriate behaviors that will shield them from online privacy threats. Following the common practice of adding an e-, an i-, or a cyber- to denote the online version of a familiar concept, we call ours *i*-Safety. The result is an intentional double entendre, the *i* signifying *i*nformation but also highlighting the role that the *i*ndividual must play to protect one's *i*nformation and the network at large. The *i*-Safety model is a social cognitive approach that highlights the role of consumer self-efficacy or confidence for privacy protection enactment as a moderator of the motivating effects of privacy concern. We use the *i*-Safety model to guide an experimental test of a warning label's potential benefits for consumer protection through its ability to influence consumer perceptions and subsequent privacy protection behaviors.

Privacy Concern and Protection Behaviors

Online consumers can and sometimes do take action to protect themselves. A fourth use separate e-mail addresses to avoid spam, nearly

two-thirds avoid posting their addresses on Web sites, and a like percentage use spam filters (Fallows 2005). Over two-thirds of Internet users have on occasion refused information requests, opted out of direct marketing lists or information transfers, or decided not to use a Web site or complete a purchase. Fewer but still substantial numbers selectively blocked cookies, cleared browser memories, read privacy statements, encrypted e-mails, or used anonymizing technologies (Milne, Rohm, and Bahl 2004).

Still, Internet privacy poses something of a paradox, some say even a fallacy (Goldman 2003). Surveys show that concerns about online privacy are widespread (e.g., Cyber Security Industry Alliance 2005; Milne, Rohm, and Bahl 2004; National Telecommunications and Information Administration 2000; Smith 2005a,b). Yet, privacy concerns have little overall impact on surfing habits or e-commerce participation (George 2004; Han and Maclaurin 2002; Jarvenpaa and Todd 1997; Khalifa and Limayem 2003; Miyazaki and Krishnamurthy 2002). Concerns had relatively weak positive relationships to privacy protection behaviors in two studies (Milne and Culnan 2004; Milne, Rohm, and Bahl 2004) but an inverse relationship in another (Chen and Rea 2004). Internet users willingly divulge personal information to obtain "free" information, personalized content (Pastore 1999), customized discounts (White 2004), prizes, loyalty program memberships (Earp and Baumer 2003), cajoling interactions with automated shopping "agents" (Berendt, Gunther, and Spiekermann 2005), or some other form of "fair exchange" (Culnan and Bies 2003). Thus, although online privacy is undeniably a "concern," one might well ask if it really influences a consumer's privacy protection behaviors.

Privacy Policies and Third-Party Seals

Whether consumer privacy concerns have any practical impact is still open to question, but they undeniably have had a political impact. In response, the FTC (2000) has supported fair information practice standards that call for *notice* of the information that is being collected, *access* to the data that are collected, *choice* about the use of the information, and reasonable assurance of the *security* of the information. Studies generally confirm that Web sites bearing privacy statements at least partially comply with the FTC guidelines (reviewed by Milne and Culnan 2002; Peslak 2005).

The FTC also supports third-party seal certifications as part of a self-regulatory approach. Web sites may participate in privacy seal programs such as TRUSTe that assure consumers of the privacy policy's veracity and compliance with FTC fair information practice standards. The premise of privacy seals such as TRUSTe and BBBOnline is widely misunderstood

(Miyazaki and Krishnamurthy 2002; Rifon, LaRose, and Choi 2005; Turow 2003); they do not assure the user's privacy but only vouch for the accuracy of the site's privacy policy, and even that is arguable (cf. Perfectly Private 2001). Indeed, many do not read privacy policies (Milne and Culnan 2004), a behavioral prerequisite for seal programs to protect consumers. The process for obtaining seal approval and the ability to "click to verify" are also widely misapprehended (Moores 2005). There is mixed evidence about the ability of seals to inspire trust. When privacy seals were manipulated in isolation from other privacy variables, they had no effect on trust (McKnight, Kacmar, and Choudhury 2004). Other evidence suggests that consumers heuristically (Petty, Cacioppo, and Schumann 1983), and inaccurately, use privacy seals to signal trust, less personal data collection, and fewer privacy violations (Rifon, LaRose, and Choi 2005) and that seals encourage both personal information disclosure and participation in e-commerce (Miyazaki and Krishnamurthy 2002). What of those who choose not to rely on privacy seals? While over four-fifths of Internet users sometimes read privacy policies at the sites they visit, fewer than 5% always read them (Milne and Culnan 2004; Privacy Leadership Initiative 2001). For those who do make the effort, the complexity and mixed messages (cf. Anton and Earp 2001) of privacy disclosure statements are daunting. Nearly a third of Internet users had difficulty understanding the privacy statements posted by Web proprietors, and two-fifths complained that they did not want to take the time to read them (Privacy Leadership Initiative 2001).

We question whether the fair information practice standards are still sufficient. Consumer confusion and the increasing presence of privacy violation attempts (spam has increased eightfold and identity thieves have made significant inroads on the Internet in the years since the FTC first established the standards) warrant the exploration of an alternative or a supplement to notice standards. We suggest that privacy policies and seals do not provide adequate information for consumer comprehension of the possible outcomes of their personal information sharing, nor do they motivate consumers to take protective actions. A different perspective is needed to inform consumers and prompt them to consider the potential consequences, positive and negative, that are associated with personal information disclosures. We suggest that a type of warning label be introduced to the present self-regulatory system.

Privacy Warning Labels

To enact self-protective behaviors, consumers must have accurate knowledge as well as confidence in their ability to take appropriate

precautions. Product warnings are widely used to inform consumers about the safe use of potentially dangerous products. In general, product warning labels appear to increase compliance with safe behaviors (Argo and Main 2004; Cox et al. 1997); in a small percentage of instances, they may decrease safe behavior. However, estimates of compliance with product warnings varied considerably across the studies included in the meta-analyses of Cox et al. (1997) and Argo and Main (2004). Each attributed this variance to the probable interactions among the warning, the product, the usage situation, and the user, that is, essentially a lack of control over effects moderators, and called for more studies evaluating the conditions that influence warning effects.

A warning label model for privacy notice is appropriate given the risk/benefit trade-offs demanded by e-commerce for consumer participation. Consumers use the Internet for many reasons including shopping, purchasing, and general information search. Yet, to have access, one must allow a level of interaction with most sites that includes the placement of cookies and the further volitional disclosure of personal information. Privacy notices, the presentation of a Web site's privacy policies, are notoriously incomprehensible (Milne, Culnan and Greene 2006), discourage their own use (Milne and Culnan 2004), and often contain assurances to lull consumer disclosures (LaRose and Rifon 2006).

A privacy warning label can summarize the information practices of a Web site and provide balanced information about the outcomes associated with each practice. The benefit and risk outcomes associated with each information practice can be itemized and presented in a way to facilitate comprehension of privacy risks and reduce an overreliance on privacy seals as heuristic safety signals. Consistent with Mazis' (1997) contention that applied policy research can and should be theory based, a privacy warning can be developed, appreciated and evaluated in the context of a theory of privacy behavior. The *i*-Safety model provides the foundation for testing the effects of that label, as well as the potential moderating effects of user characteristics. The following section develops hypotheses for Web site privacy warning effects.

UNDERSTANDING PRIVACY BEHAVIOR: THE *I*-SAFETY MODEL

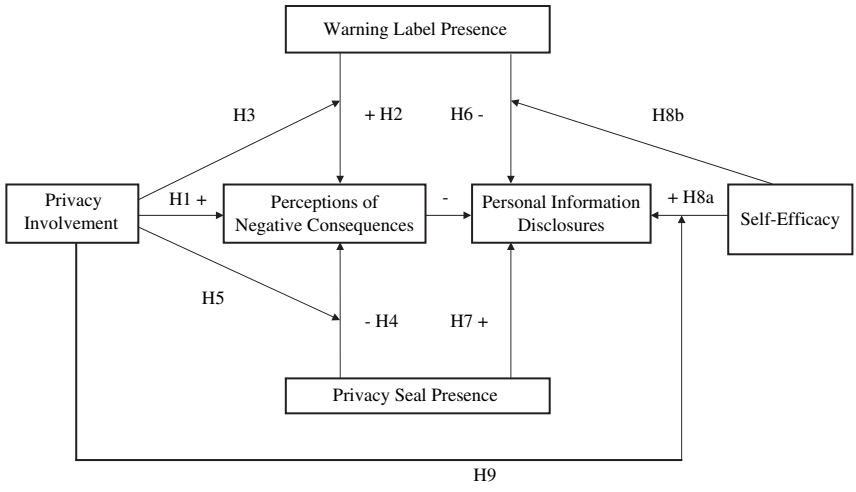
The present research contends that privacy protection behavior may be explained by social cognitive theory (SCT). Likewise, attempts to influence that behavior may be understood through theories of consumer cognitive response to persuasion attempts (Celsi and Olson 1988; Petty, Cacioppo,

and Schumann 1983). In so doing, we propose a model of privacy protection behavior that integrates privacy concern, risk, and trust using well-established cognitive constructs, mainly self-efficacy, and involvement. We expect that personal information disclosures will be a function of the consumer's assessment of the risks of those disclosures. However, those risk perceptions will be a function of privacy involvement, the consumer's motivation to notice and process a statement of that risk. In addition, risk perceptions will be a function of self-efficacy, an assessment of one's ability to cope with that risk (see Figure 1).

SCT (Bandura 1986) explains that outcome expectations, defined as judgments of the likely consequences of a behavior, provide incentives for enacting behavior. Positive outcomes encourage behavior, while expectations of negative outcomes provide disincentives. Self-efficacy, or belief in one's capability to organize and execute a particular course of action to achieve important attainments, determines whether sufficient levels of effort will be invested to achieve successful outcomes when one is already motivated to do so.

Applying this theory, outcome expectations focus on the consequences of behavior, for example, that spam attacks result from third-party disclosures or that shopping is more convenient when a site "knows" your name. Outcome expectations may be shaped by personal experience (enactive learning in social cognitive terms) with privacy violations, by our observation

FIGURE 1
Effects of Privacy Cues on Personal Information Disclosures



of the privacy behaviors enacted by others (vicarious learning), or by persuasion attempts such as those found in Web site privacy notices. Consumers' reluctance to disclose information that is personally identifying is theoretically attributable to corresponding differences in the perceived severity of negative consequences (risks) of disclosure. Since personally identifying disclosures are required to complete online transactions, there should be a concomitant effect on online buying behavior.

However, only expectations about the negative consequences of complying with the demands of a specific site, not generalized privacy concerns (as in Miyazaki and Krishnamurthy 2002), should have this effect. In SCT, it is vital to match the expectations to the specific behavior in question. Vague concerns about privacy may reflect expectations of negative outcomes but are at best an imprecise and possibly confounded measure of the concept. In social cognitive terms, concern may also confound negative expected outcomes and self-efficacy. Someone may expect negative outcomes from supplying consumer information but not be concerned because they know how to avert the danger, such as by maintaining multiple online identities. Indeed, this was the essence of the explanation that Chen and Rea (2004) gave for their results. The paradoxical failure to observe a direct relationship between privacy concerns and buying behavior may result from a failure to conceptualize and operationalize privacy in terms of known determinants of behavior.

Thus, we expect that the presence of a privacy warning label that clearly presents the possible negative consequences associated with personal disclosures will increase expectations of negative outcomes and have an inverse effect on the likelihood of personal disclosures. Previously, privacy concern was found to be correlated to enactment of a composite measure of several privacy protections, including withholding of personal information (Milne, Rohm, and Bahl 2004). Here, we propose that there is a causal relationship between concerns, more properly conceived as expected negative consequences, and nondisclosure.

Perceptions of Negative Consequences

Theories of consumer cognitive processing become salient when formulating interventions to change beliefs about the consequences of privacy behavior. "Privacy concern" might also imply a heightened state of attentiveness to privacy protection; as such, it is essentially the same as ego-involvement (Sherif and Cantril 1947), enduring involvement, and subsequent felt involvement (Celsi and Olson 1988). The greater the consumer's involvement, the more likely the individual will focus attention on the

message, actively process it (Celsi and Olson 1988), and resist persuasion attempts (Petty, Cacioppo, and Schumann 1983). An individual who is not involved with a message is not likely to attend to it or actively process it and is more open to persuasion through the use of peripheral cues that are easily recognizable, familiar, and attractive.

Thus, those highly involved in privacy issues are likely to seek out and attend to privacy statements, read them carefully, resist the attempts of Web site proprietors to convince them to surrender private information, and attend closely to information about privacy threats. In survey studies, such individuals have been variously characterized as privacy fundamentalists or alarmed Internet users (Sheehan 2002).

Following prior research (Miyazaki and Krishnamurthy 2002; Rifon, LaRose, and Choi 2005), privacy seals should encourage disclosures. And, since consumers commonly misconstrue privacy seals as assurances of privacy protection, rather than merely assurances of the accuracy of privacy statements (Turow 2003), their presence should lessen expectations of negative privacy outcomes. However, those with low privacy involvement, who might be said to be unconcerned (Sheehan 2002), are likely to rely on peripheral cues such as privacy seals and to be more susceptible to the assurances of Web site proprietors, while ignoring warnings about privacy dangers. Argo and Main (2004) also note the importance of differentiating warning effects on the basis of intentional versus incidental exposure. In SCT, involvement might be construed as an indicator of active self-observation, situations in which consumers are highly attentive to their own behavior and actively judging it against personal and social norms (Bandura 1991). We would therefore expect highly involved consumers to be more attentive to the negative consequences of privacy disclosures.

H1: Privacy involvement will be directly related to expectations of negative privacy outcomes.

H2: Consumers who view a privacy warning label will report stronger expectations of negative consequences than consumers who do not view a warning.

H3: Consumers with low privacy involvement will be more responsive to the presence of a privacy warning label exhibiting stronger expectations of negative consequences than those who do not see a warning label.

Familiar sources that are viewed as credible, that is, trustworthy, attractive, and possessing expertise (Atkin and Block 1983; Ohanian 1989), are also used heuristically to assess the meaning of the message, most especially by those who have low involvement. Source credibility thus parallels

the concept of e-trust in Internet research (Gefen, Karahanna, and Straub 2003), a quality of Web sites that is built through repeated transactions or community relationships. Following prior research, e-trust (Chadwick 2001) should directly encourage personal information disclosures. An interaction with involvement should also be found. When consumers have no direct information about the trustworthiness of a site, they may infer it from the certification supplied by the seal authority.

H4: Privacy seal presence will lower expectations of negative privacy outcomes.

H5: Privacy involvement will moderate the effects of seal presence on outcome expectations: those with low privacy involvement will have higher expectations of negative privacy outcomes with a warning label present, but those with high privacy involvement will not be affected.

Information Disclosures

Logically, we expect that the privacy information would influence disclosure intentions and also be moderated by the individual characteristics of self-efficacy and involvement.

H6: Privacy warnings will decrease disclosure intentions.

H7: Privacy seals will increase disclosure intentions.

The findings of Rifon, LaRose, and Choi (2005) indicate that greater consumer confidence may work against the intended effects of warnings. Individuals who are confident are less likely to seek out risk-related information resulting in more risky behaviors. An interaction between consumer information about negative consequences and self-efficacy may also be expected (Argo and Main 2004). Internet users with high degrees of self-efficacy should be more willing to discount negative consequences when providing personal information than those with low self-efficacy, because they perceive themselves as being able to cope with any negative outcomes. Since the amount of online experience is directly related to Internet self-efficacy (Eastin and LaRose 2000), that would explain the positive relationship between experience and information disclosure (Rainie 2001). Self-efficacy is theoretically directly related to behavior, and the relationship is reciprocal (Bandura 1997). Persons who believe in their ability to control private information should be more likely to engage in behaviors that preserve privacy than those with low self-efficacy.

H8a: Privacy self-efficacy will be directly related to the amount of personal information disclosed.

H8b: Privacy self-efficacy will moderate the influence of the privacy warning label. Negative consequence information will have a greater negative effect on personal information disclosure among those with low self-efficacy than among those with high self-efficacy.

We also expect that self-efficacy would moderate the influence of privacy involvement on personal information disclosures:

H9a: Among those with high privacy involvement, the presence of a privacy seal will increase the disclosure of personal information when self-efficacy is high but have no effect when self-efficacy is low.

H9b: Among those with low privacy involvement, the presence of a privacy seal will increase the disclosure of personal information more when self-efficacy is low than when it is high.

RESEARCH METHODS

Respondents

Two hundred and twenty-seven participants were recruited from undergraduate classes in telecommunication, advertising, and packaging at a major Midwestern University. Consistent with the composition of those classes, 67% of the respondents were female, 33% were male and they had a median age of nineteen years. The mean time spent on the Internet on a typical weekday was three hours and forty minutes. College student–aged (eighteen to twenty-four years) participants represent a vulnerable and relevant Internet user group. Young adults experience the greatest risk of privacy violations. In 2005, the FTC reported that the 18- to 29-year-old segment reported the highest incidence of identity theft (29% of all complaints) and 25% of all Internet fraud (FTC 2005). Even worse, they are more likely to be unconcerned or pragmatic than wary or alarmed about their privacy (Sheehan 2002). They also represent an important consumer demographic, Generation Y, to online retailers. They have the highest Internet use of any age group (Fox and Madden 2005; U.S. Department of Commerce 2004). In addition, their online buying and purchasing behavior is representative of a wide range of users (Fox and Madden 2005).

Design and Data Collection Procedure

A 2×2 between-subjects experimental design was created by manipulating the presence/absence of a privacy warning label and the presence/absence of a privacy seal on a stimulus Web site. Data were collected in two, separate online sessions that respondents attended through their own personal computers. General background information about the respondents' demographic characteristics and Internet usage as well as the privacy involvement and privacy self-efficacy measures described below were administered during the first session. Privacy involvement was split at its median value to assign equal numbers of respondents to high- and low-involvement groups. Respondents were randomly assigned to one of four groups within each involvement level. Respondents were recontacted via e-mail with the URL for the appropriate condition, where the privacy statement and seal manipulations and the posttest containing the dependent variables and trust measures were found.

Operational Measures

The dependent variables were the expected negative outcomes of personal information disclosures, intentions to supply personally typifying and personally identifying information. The measures appear in Table 1. Behavioral intentions have been shown to be a reliable predictor of behavior across a wide range of domains (Ajzen and Fishbein 1980) and provide an efficient means of assessing behavioral outcomes. Intentions to supply personally typifying information to the Web were operationally defined by a 3-item index of likelihood scales ($\alpha = .89$, mean $= 18.43$, SD $= 3.41$), while intentions to supply personally identifying information ($\alpha = .87$, mean $= 19.58$, SD $= 7.55$) contained six items. The roster of information items was drawn from Cranor, Reagle, and Ackerman (1999) and subjected to principal components factor analysis, with varimax rotation, to clearly distinguish the two types. Buying intentions ($\alpha = .87$, mean $= 7.80$, SD $=$ 2.84), consisting of two 7-point agree–disagree (7 = strongly agree, 1 = strongly disagree) items previously reported (Gefen 2002).

The 6-item expected negative outcomes scale ($\alpha = .90$, mean $= 23.04$, SD $= 6.66$) measured the perceived likelihood (on a 7-point scale, scored 7 for very likely, 1 for very unlikely) of negative consequences occurring as a result of providing personal information to the Web site associated with the privacy statement the respondent had just read. Candidate items were developed from focus-group interviews previously conducted with respondents drawn from the same general student population.

TABLE 1
Scale Items

Intentions to Disclose Personally Typifying Information
My favorite snack food
My favorite TV program
My favorite hobby
Intentions to Disclose Personally Identifying Information
My last name
My street address
My telephone number
My email address
My credit card number
My social security number
Buying Intentions
I would use my credit card to purchase from this web site
I am very likely to buy products from this web site
Negative Outcomes
I'll be the victim of an online scam
Information will be captured that could be used against me in my future life
Someone will hack into the site and steal my personal information
Someone will use the information to harass me
I'll get unauthorized charges on my credit card
My identity will get stolen
Privacy Involvement
Matters to me; Doesn't matter to me; Of no concern; Of concern to me; Irrelevant; Relevant; Important; Not important
1. It's easy to figure out which sites you can trust on the Internet; I am confident I know how to protect my credit card information online; I know how to identify sites with secure servers; I know how to evaluate online privacy policies; It's easy to set up dummy email account to shield my identity; I know how to change the security settings of my browser to increase privacy; I know how to use a virus-scanning program; I am able to protect myself against the release of personal information; I know how to block unwanted E-mails; Overall, I am confident that I can protect my privacy online.
2. I expect that the advice given by this web site is their best judgment; I can count on this web site to be sincere; I expect that this web site is ready and willing to assist and support me; I expect that this web site has good intentions toward me; I expect this web site's intentions are benevolent; I expect that this web site puts customers' interests before their own; I expect that this web site is well meaning.

One blocked and one measured independent variables were developed from questionnaire items. Privacy involvement ($\alpha = .85$, mean = 7.40, SD = 3.94) was a 4-item additive index of 7-point semantic differential (scored +3 for responses indicating involvement and −3 for items indicating noninvolvement (Ohanian 1989). Privacy self-efficacy ($\alpha = .83$, mean = 42.06, SD = 10.20) consisted of ten items (with the 7-point Likert-type agree–disagree scale format) and was designed to measure a respondent's perceived ability to protect their privacy on the Internet. It was split at its median value of 42 into high (coded as 1) and low (coded as 0) self-efficacy for the purpose of analysis of variance. Candidate items were again drawn from previous focus-group interviews.

Stimulus Materials: Web Site

Four stimulus Web sites were created for a fictitious company, Amazing-deals.com. The stimulus Web sites contained Amazon.com's privacy policy statement from April 2003. Amazon.com was chosen because it is a widely visited electronic commerce site and because it contains a wide range of both proprivacy assurances and antiprivacy threats. To avoid confounding with the familiarity of the Web site, all references to Amazon.com and to proprietary terms used by Amazon.com were deleted.

Privacy Warning

The privacy warning–label treatment condition added a table headed "Your Privacy Risk Summary." The study was designed to examine first if privacy warnings have potential value for informing and protecting consumers about the risks associated with information practices and second the psychological or consumer conditions under which the warning may be effective. Hence, the label was created to be vivid and conspicuous. The warning label appeared at the beginning of the privacy statement, making it the first thing the respondents saw. It was immediately followed by the text of the privacy policy. Consistent with the recommendations of Bettman, Payne, and Staelin (1986) for hazardous label design, the privacy warning label presented privacy practices visually aligned with their benefits and risks and in contrasting colors (see Appendix). Each of the three columns containing information about Web site practices and associated benefits and risks was presented in a different-color text. To facilitate comprehension, the warning "chunked" related practices, benefits and risks visually within each row, and provided benefits within one column and risks within another. The first column (blue text) had the subheading of "What We Do" and listed actions the Web page takes that affect user privacy (e.g., Record your credit card number). The second column (green text) was subtitled "How You Benefit" and listed advantages that corresponded with the actions from the first column (e.g., Convenient on-line shopping). The final column (red text) contained the title "What You Risk" and listed the negative consequences associated with the action in the first column (e.g., unauthorized credit charges). The privacy warning label contained a total of thirteen actions with corresponding benefits and risks. All the actions and benefits contained within the warning label were found in the text of Amazon.com's privacy policy. The risks were added by the experimenters, based on a focus-group exercise in which respondents were asked to circle phrases in the Amazon privacy statement which raised

concerns about privacy and their perceptions of the ultimate personal consequences of those policies.

Data Analysis

Data were analyzed using the SPSS statistical package, version 11.5 (SPSS, Inc. 2002). Pearson product-moment correlations were used to test hypothesis about bivariate relationships between variables. The general linear model procedure was used to examine relationships between the manipulated and the measured independent variables, the interactions between them, and the dependent variables. A separate analysis was conducted for each of the four dependent variables (negative outcome expectations, information disclosure intentions, buying intentions, and trust). An overall F test was performed for each dependent variable, and individual hypotheses were tested by examining the pertinent main effects and interaction effects, below. Fourth-order interactions were suppressed to meet minimum cell-size requirements.

RESULTS

Consumer information privacy variables were significantly related to expectations of negative privacy outcomes, $F(7, 219) = 4.13$, $p < .001$, and intentions to disclose personally identifiable information, $F(14, 211) = 2.79$, $p < .001$ (Table 2).

Expectations of Negative Outcomes

As predicted by H1, those with high privacy involvement were much more likely to expect negative privacy outcomes than those with low involvement, $F(1, 219) = 18.93$, $p < .001$. The expected main effects of the privacy warning label (H2) and privacy seal (H4) were not confirmed, nor was the moderating effect of involvement on privacy warning label presence (H3). Privacy involvement did not moderate the effects of a privacy seal, disconfirming H5 as well. However, an unexpected privacy warning label $\times$ privacy seal interaction was found, $F(1, 219) = 4.94$, $p < .05$. In the absence of a privacy seal, the privacy warning box greatly increased expectations of negative outcomes, but when a privacy seal was present, privacy warnings slightly decreased expectations of negative outcomes.

TABLE 2
Tests of Between-Subjects Effects on Personal Information Disclosure Intenstions

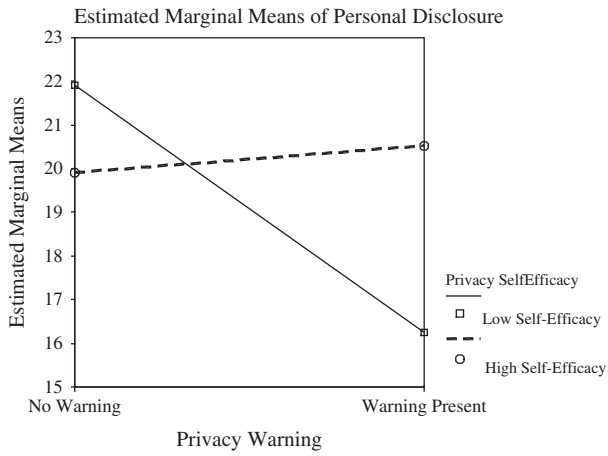
Source	Type III Sum of Squares	df	Mean Square	*F*	Sig.
Corrected model	2,007.761[a]	14	143.412	2.793	.001
Intercept	83,779.453	1	83,779.453	1,631.761	.000
Self-efficacy	62.635	1	62.635	1.220	.271
Involvement	55.421	1	55.421	1.079	.300
Privacy box warning	323.314	1	323.314	6.297	.013
Privacy seal	403.304	1	403.304	7.855	.006
Self-efficacy × involvement	10.270	1	10.270	.200	.655
Self-efficacy × warning	554.062	1	554.062	10.791	.001
Self-efficacy × seal	6.258	1	6.258	.122	.727
Involvement × warning	90.139	1	90.139	1.756	.187
Involvement × seal	16.120	1	16.120	.314	.576
Warning × seal	52.768	1	52.768	1.028	.312
Self-efficacy × involvement × warning	12.922	1	12.922	.252	.616
Self-efficacy × involvement × seal	371.921	1	371.921	7.244	.008
Self-efficacy × warning × seal	.172	1	.172	.003	.954
Involvement × warning × seal	36.049	1	36.049	.702	.403
Error	10,884.710	212	51.343		
Total	99,882.685	227			
Corrected total	12,892.471	226			

[a] $R^2 = .156$ (adjusted $R^2 = .100$).

Disclosure Intentions

As predicted, there was a negative main effect (H6) for privacy warnings, $F(1, 212) = 6.30$, $p < .05$, and a positive main effect (H7) for privacy seals, $F(1, 212) = 7.86$, $p < .01$, on disclosure intentions. There was no direct relationship between privacy self-efficacy and disclosure (H8a). The interaction (H8b) between consumer privacy warnings and privacy self-efficacy was confirmed, $F(1, 212) = 10.79$, $p < .001$ (Figure 2), and was the type expected: privacy warning labels had no effect on those with high self-efficacy but decreased the amount of personally identifiable information that those with low self-efficacy were willing to divulge. As predicted, a three-way interaction among privacy seals, privacy involvement, and self-efficacy was observed, $F(1, 212) = 7.24$, $p < .01$ (Figures 3 and 4). Among those with high privacy involvement, seals had no effect on those with high privacy self-efficacy, but seals increased disclosures among those with low privacy self-efficacy, confirming H9a. Among those with low privacy involvement, just the opposite was true: seals had no effect on respondents with low privacy self-efficacy but increased disclosures among those with high privacy self-efficacy, supporting H9b.

FIGURE 2
Plots of Means for Warning × Self-Efficacy Interaction



DISCUSSION

Privacy, indeed, does matter and can influence consumer privacy behaviors. When information about potential negative outcomes of privacy disclosures was communicated to consumers, it made them less inclined to supply personally identifying information and less likely to purchase

FIGURE 3
Plot of Means for Self-Efficacy × Seal Interaction for Low Involvement

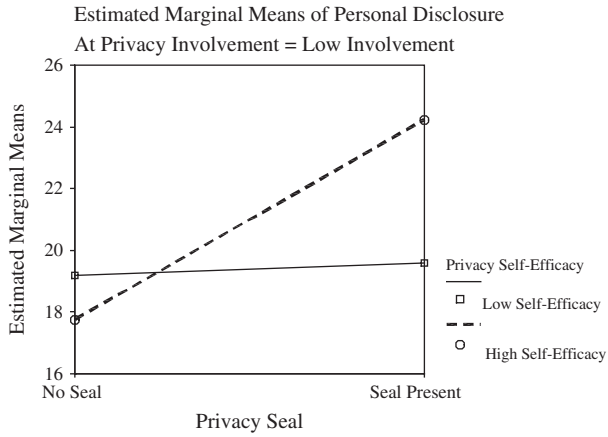
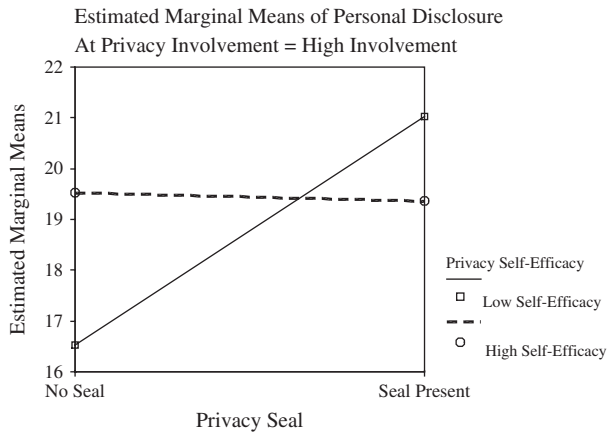


FIGURE 4
Plot of Means for Self-Efficacy × Seal Interaction for High Involvement



products from a Web site that puts their privacy at risk. Privacy warnings may increase *i*-Safety, the enactment of information self-protection by online consumers.

However, consumers differ in their perceived abilities to protect themselves, their privacy self-efficacy beliefs, and this may be the key to unraveling the privacy paradox. While privacy self-efficacy had no direct effect on self-disclosure, it moderated the effects of privacy warning presence, consumer information about negative outcomes of privacy disclosures—what have variously been called privacy concerns, fears, or risks. Highly self-efficacious consumers were unaffected by information about negative consequences, but those with little self-efficacy were unlikely to supply personally identifying information when they were made aware of the potentially harmful side effects of such disclosures. This interaction effect may well be obscured in cross-sectional survey studies where consumers with differing levels of privacy self-efficacy are lumped together. And, the studies that seemed to indicate that privacy did not matter may rather provide evidence that many consumers are unaware of their true privacy risks or are (over) relying on third-party certifications and other peripheral cues to allay their concerns. In other words, privacy does matter but not when consumer confusion and misinformation reign.

The effects of privacy seals and whether or not they are in consumers' best interests is an intricate question. The finding that privacy seals cause disclosure is in itself somewhat disturbing. Contrary to popular belief (cf. Turow 2003), seals do not guarantee privacy, only that the statements about

privacy by Web site proprietors are accurate. In fact, sites with seals are perhaps bigger threats to personal privacy than those without them in that they engage in more intrusive information practices (LaRose and Rifon 2006). Here, involvement and self-efficacy worked in concert to mediate the effects of privacy seals. Seals encouraged disclosures either when privacy involvement was high and self-efficacy was low or when involvement was low but self-efficacy was high. To put these findings in their harshest light, they indicate that seals help encourage disclosures from two particularly vulnerable types of consumers: those who worry about online privacy but do not know how to protect themselves and those who know how to protect themselves but are careless about doing so. Seals may function to conceal the true risks of privacy invasions while winning trust with peripheral cues that give only the appearance of privacy protection but not its substance. Those with low privacy self-efficacy are unlikely to become more trusting of sites with seals; so, at least the effects are limited to those who are perhaps best able to overcome the negative personal effects of deception.

Two characteristics of the study, the college student sample and forced exposure experimental setting, suggest that the effects of privacy information observed in this study may not represent effects in the general population. Forced exposure to privacy policy statements was used, while few consumers read these policies or are aware of their significance (Turow 2003). The results may exaggerate the effects of privacy seals and warnings, at least in the current online environment in which privacy protection information is not made salient to the consumer. However, the purpose of the study was to identify the possible value of a privacy warning label. Internal validity must be the prime concern for this first study. As such, the label must be obvious and available. In the meta-analysis findings of Cox et al. (1997), student samples exhibited greater compliance with product warnings than adult samples, but no age differences were found by Argo and Main (2004). On the other hand, young consumers are less willing to engage in information safety protection online (Milne, Rohm, and Bahl 2004) than are older consumers but also more likely to read privacy policies (Earp and Baumer 2003). Future studies should continue to examine the value of explicit privacy warnings with different populations and more refined stimulus materials.

We argue that *i*-Safety information should be made more salient and that both the current FTC guidelines, and voluntary seal programs that embody them, do not go far enough. Privacy statements should clearly describe the end effects of a site's privacy policies. Ideally, context-dependent notifications (see Berendt, Gunther, and Spiekermann 2005; Liu et al. 2005),

complete with recommended self-protective actions that take into account the safety resources on the consumer's computer (e.g., "run spybot after you visit this site") and the consumer's competency level (e.g., "to learn how to download a spyware removal program, click here"), might appear when risky actions are about to be taken.

The results of this study provide support for the development of privacy warning labels, much like those developed for food nutrition labels through the Nutrition Labeling and Education Act of 1990. At the time of this writing, the FTC was considering recommendations for more compact and clear privacy policies. The results of this study support that effort. The warning used in this study is a preliminary attempt to summarize and present the salient risks and benefits associated with information practices. The study was not a formative test of its design but of its potential for the facilitation of consumer-informed choice to participate in Web site information practices, particularly the disclosure of personal information.

Theoretical notions of privacy concerns should be further developed. The premise of the present research was that privacy concerns reflect, albeit imprecisely, expected negative outcomes of information disclosure. Given the large body of privacy research that is predicated on privacy concerns, it would be helpful to further explore the relationship of privacy concerns to variables that are known to predict behavior, such as expected outcomes and self-efficacy, and to constructs that are found in theories of consumer information processing, including involvement, fear, and anxiety. By conceptualizing privacy as a safety behavior and connecting it to both SCT and consumer information processing, we can connect *i*-Safety to a wide range of research about risky behavior and health communication in particular. For example, protection motivation theory (see Floyd, Prentice-Dunn, and Rogers 2000 for a recent review) is rooted in SCT and suggests a wide range of unexplored variables and intervention strategies that may be applied to the *i*-Safety problem. The findings also support the adoption of a social cognitive paradigm to the study of effects of a variety of product warnings. The *i*-Safety model can be generalized to other areas for safe product use.

Online privacy does matter to consumers, but consumers' involvement with privacy issues and their perceptions of their own ability to protect privacy affect the behavioral impact of consumer information. In the interest of consumer protection as well as collective online safety, Web sites should display more clear and conspicuous information about their information practices, including explicit warnings of the risks they pose to their users.

Appendix: Privacy Warning Label

Your Privacy Risks and Benefits Summary

What We Do	How You Benefit	What You Risk
Record your email address.	Personal product alerts, order status updates, respond to your requests.	Unwanted commercial email.
Record your name and address.	Personal shopping lists and gift registries, provide and rate customer reviews, participate in contests and chat, share information with friends.	Unwanted commercial email, personally harassing email, identity theft.
Receive notification when you open email from us.	Make emails from us more useful and interesting.	More commercial email from us.
Record your credit card number.	Convenient online shopping.	Unauthorized credit card charges.
Record you list of associates.	Make your own shopping circle. Chat with your friends at our site.	Law enforcement may obtain the list of your associates.
Record your social security number.	Access to our financial services.	Unauthorized credit card charges, identity theft.
Leave cookies on your computer.	One Click purchasing, personalized greetings, save items between visits.	Banner ads and commercial email.
Share your personal information with third parties.	Better customer service, speedier delivery, access to our affiliates.	Unwanted commercial email.
Exchange information with law enforcement and credit bureaus.	Fraud protection, credit risk reduction.	Your credit rating could suffer, erroneous information.
Match information about you from third parties.	Avoid unnecessary messages. Correct our records, speedier delivery.	Banner ads and commercial email.
Track the sites you come from and go to.	We understand you better to serve you better.	Law enforcement may obtain the records.
Keep track of your movements on our site.	Improve the design of our stores to serve you better.	Commercial messages from us.
Keep track of your purchases.	Customize future shopping. Personal purchase summaries. Match you with other shoppers.	Commercial pitches from us, Law enforcement obtain the records.

REFERENCES

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

Antón, Annie I., and Julia B. Earp. 2001. Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems. *Recent Advances in Secure and Private E-Commerce*. Kluwer Academic Publishers, Dordecht, 2001.

Argo, Jennifer J., and Kelley J. Main. 2004. Meta-Analysis of the Effectiveness of Warning Labels. *Journal of Public Policy & Marketing*, 23 (2): 193–208.

Atkin, Charles, and Martin Block. 1983. Effectiveness of Celebrity Endorsers. *Journal of Advertising Research*, 23(February/March): 57–61.

Bandura, Albert. 1986. *Social Foundations of Thought and Action*. Englewood Cliffs, NJ: Prentice-Hall.

———. 1991. Social Cognitive Theory of Self-Regulation. *Organizational Behavior and Human Decision Processes*, 50 (22): 248–287.

———. 1997. *Self-Efficacy: The Exercise of Control*. New York: W.H. Freeman.

Berendt, Bettina, Oliver Gunther, and Sarah Spiekermann. 2005. Privacy in E-commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM*, 48 (4): 101–106.

Better Business Bureau. *New Research Shows That Identity Theft Is More Prevalent Offline with Paper than Online*. Better Business Bureau, 2005. http://www.bbb.org/alerts/article.asp?ID=565 (retrieved June 28, 2005).

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

Brightmail. 2004. *Brightmail Intensifies the Global Fight Against Spam*. http://www.e-consultancy.com/newsfeatures/154287/brightmail-intensifies-the-global-fight-against-spam.html (retrieved June 26, 2005).

Celsi, Richard. L., and Jerry C. Olson. 1988. The Role of Involvement in Attention and Comprehension Processes. *Journal of Consumer Research*, 15 (2): 210–224.

Chadwick, Scott A. 2001. Communicating Trust in E-commerce Interactions. *Management Communication Quarterly*, 14 (4): 653–658.

Chen, Kuanchin, and Alan I. Rea Jr. 2004. Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. *The Journal of Computer Information Systems*, 44 (4): 85–92.

Consumer Reports. 2004. Protect Yourself Online. *Consumer Reports,* September, 16.

Cox, Eli P. III, Michael S. Wogalter, Sara L. Stokes, and Elizabeth J. Tipton Murff. 1997. Do Product Warnings Increase Safe Behavior? A Meta-Analysis. *Journal of Public Policy & Marketing*, 16 (2): 195–204.

Cranor, Lori F., Joseph Reagle, and M. S. Ackerman. 1999. Beyond Concern: Understanding New Users' Attitudes About Online Privacy. In *AT&T Labs-Research Technical Report*. http://www.tprc.org/ABSTRACTS99/CRANORPAP.PDF.

Culnan, Mary J. and Robert J. Bies. 2003. Consumer Privacy: Balancing Economic and Justice Considerations. *The Journal of Social Issues*, 59 (2): 323–361.

Cyber Security Industry Alliance. 2005. *Internet Security Voter Survey*. https://www.csialliance.org/home (retrieved June 26, 2005).

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

Eastin, Matthew. S. and Robert LaRose. 2000. Internet Self-Efficacy and the Psychology of the Digital Divide. Review of Reviewed Item. *Journal of Computer Mediated Communication*, 6 (1), http://www.asusc.org/jcmc/vo16/issue1/eastin.html.

Fallows, Deborah. 2005. *CAN-SPAM a Year Later*. http://www.csialliance.org/resources/pdfs/CSIA_Internet_Security_Survey_June_2005.pdf.

Federal Trade Commission (FTC). 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace*. http://www.ftc.gov/.

———. 2005. *Consumer Fraud and Identity Theft Complaint Data: January–December 2005*. http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

Floyd, Donna L., Steven Prentice-Dunn, and Ronald W. Rogers. 2000. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30 (2): 407–429.

Fox, Susannah and Mary Madden. 2005. *Pew Internet and American Life Project*. http://www.pewinternet.org/pdfs/PIP_Generations_Memo.pdf.

Gefen, David. 2002. Reflections on the Dimensions of Trust and Trustworthiness Among Online Consumers. *Database for Advances in Information Systems*, 33 (3): 38–53.

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

George, Joey F. 2004. The Theory of Planned Behavior and Internet Purchasing. *Internet Research*, 14 (3): 198–212.

Goldman, Eric. 2003. The Internet Privacy Fallacy. *Computer and Internet Lawyer*, 20 (January): 20.

Goodwin, Cathy. 1991. Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing*, 10 (1): 149–166.

Han, Peter, and Angus Maclaurin. 2002. Do Consumers Really Care About Online Privacy? *Marketing Management*, 11 (38): 35–38.

Jarvenpaa, Sirrka L. and Peter A. Todd. 1997. Consumer Reactions to Electronic Shopping on the World Wide Web. *International Journal of Electronic Commerce*, 1 (2): 59–88.

Khalifa, Mohamed and Moez Limayem. 2003. Drivers of Internet Shopping. *Communications of the ACM*, 46 (12): 233–239.

LaRose, Robert and Nora Rifon. 2006. Your Privacy Is Assured—Of Being Invaded: Websites With and Without Privacy Seals. *New Media and Society*, 8 (6): 1009–1029.

Lee, Laurie T. and Robert LaRose. 1994. Caller ID and the Meaning of Privacy. *Information Society*, 4: 247–266.

Liu, Chang, T. Jack Marchewka, June Lu, and Chun-Sheng Yu. 2005. Beyond Concern—A Privacy-Trust-Behavioral Intention Model of Electronic Commerce. *Information & Management*, 42 (2): 289–304.

Mazis, Michael. 1997. Marketing and Public Policy: Prospects for the Future. *Journal of Public Policy and Marketing*, 16 (1): 139–143.

McKnight, D. Harrison, Charles J. Kacmar, and Vivek Choudhury. 2004. Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business. *Electronic Markets*, 14 (3): 252–266.

MessageLabs. 2005. Email Threats. http://www.messagelabs.com/.

Milne, George R., and Mary J. Culnan. 2002. Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998–2001 US Web Surveys. *Information Society*, 18 (5): 345–370.

Milne, George R., and Mary J. Culnan. 2004. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing*, 18 (3): 15–29.

Milne, George R., Mary J. Culnan, and Henry Greene. 2006. A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing*, 5 (2): 238–249.

Milne, George, R., J. Andrew Rohm, and Shalini Bahl. 2004. Consumers' Protection of Online Privacy and Identity. *The Journal of Consumer Affairs*, 38 (2): 217–232.

Miyazaki, Anthony D. and Sandeep Krishnamurthy. 2002. Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *The Journal of Consumer Affairs*, 36 (1): 28–49.

Moores, Trevor. 2005. Do Consumers Understand the Role of Privacy Seals in E-commerce? *Communications of the ACM*, 48 (3): 86–91.

National Cyber Security Alliance. 2004. AOL/NCSA Online Safety Study. https://www.csialliance.org/home.

National Telecommunications and Information Administration, ed. 2000. *Falling Through the Net: Toward Digital Inclusion*. http://www.ntia.doc.gov/ntiahome/fttn00/contents00.html.

Ohanian, Roobina. 1989. Ego Centrality as an Indicator of Enduring Product Involvement. *Journal of Social Behavior and Personality*, 4 (3): 443–455.

Pastore, Michael. 1999. Consumers Will Provide Information for Personalization. http://cyberatlas.internet.com/markets/advertising/article/0,,5941_236141,00.html (retrieved February 21, 2002).

PC Magazine. 2004. High-tech Holidays, Internet Safety Begins at Home, November. http://www.pcmag.com/article2/0,1759,1729610,00.asp.

Perfectly Private. 2001. Privacy Seals Revealed. http://www.perfectlyprivate.com/newsresources_seals.asp (retrieved January 5, 2003).

Peslak, Alan R. 2005. Internet Privacy Policies: A Review and Survey of the Fortune 50. *Information Resources Management Journal*, 18 (1): 29–41.

Petty, Richard E., John T. Cacioppo, and David Schumann. 1983. Central and Peripheral Routes to Advertising Effectiveness: The Moderating Role of Involvement. *Journal of Consumer Research*, 10 (2): 135–146.

Privacy Leadership Initiative. 2001. *Privacy Notices Research: Final Results*. https://www.bbbonline.org/UnderstandingPrivacy/library/datasum.pdf.

Rainie, Lee. 2001. *Testimony of Lee Rainie to the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce*. http://www.pewinternet.org/reports/toc.asp?Report=34 (cited February 20, 2001).

Rifon, Nora J., Robert LaRose, and Sejung Marina Choi. 2005. Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and False Assurances. *Journal of Consumer Affairs*, 39 (2): 337–360.

Sheehan, Kim Bartell. 2002. Toward a Typology of Internet Users and Online Privacy Concerns. *Information Society*, 18 (1): 21–32.

Sherif, Muzafer, and Hadley Cantril. 1947. *The Psychology of Ego-Involvement*. New York: John Wiley.

Smith, Marcia S. 2005a. In *Identity Theft: The Internet Connection*, edited by C.R. Service. Library of Congress, Congressional Research Service Report to Congress, available at http://opencrs.cdt.org/rpts/RL31408_20051019.pdf.

———. 2005b. In *Internet Privacy: Overview and Pending Legislation*, edited by C.R. Service. Library of Congress, Congressional Research Service Report to Congress, available at http://www.usembassy.it/pdf/other/RS22082.pdf.

SPSS, Inc. 2002. *Statistical Package for the Social Sciences*, Version 11.5. Chicago: SPSS.

Turow, Joseph. 2003. In *Americans and Online Privacy*, edited by A.P.P. Center. University of Pennsylvania. http://www.perfectlyprivate.com/newsresources_seals.asp.

U.S. Department of Commerce. 2004. *A National Online: Entering the Broadband Age*. http://www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.htm.

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