

**Internet Seals of Approval:
Effects on Online Privacy Policies and Consumer Perceptions**

Anthony D. Miyazaki, University of Miami
Sandeep Krishnamurthy, University of Washington

The authors, who contributed equally to this research, thank April Bowman, Sebastian Fernandez, Debbie Roth and Mahesh Shankarmahesh for assistance in data collection and processing, and David Sprott for comments on earlier versions of the paper.

NOTE: This is a penultimate version of this paper.

**Internet Seals of Approval:
Effects on Online Privacy Policies and Consumer Perceptions**

ABSTRACT

The use of Internet seal of approval programs has been touted recently as an alternative to potential legislation concerning consumer-related online privacy practices. Questions have been raised, however, regarding the effectiveness of such programs with respect to maintaining privacy standards and aiding online consumers. The authors examine these issues in a series of four studies, the first of which examines Internet seal of approval logo usage in the current marketplace. The next study applies Federal Trade Commission privacy standards to various online privacy policies in an effort to determine the ability of seal of approval program participation to act as a valid cue to a firm's state privacy practices. The last two studies are experiments designed to ascertain how online firm participation in Internet seal of approval programs affect consumers. Implications for policy and industry are also discussed.

**Internet Seals of Approval:
Effects on Online Privacy Policies and Consumer Perceptions**

Concern regarding the privacy of personal information has been declared a major obstacle of consumer participation in various online activities (Culnan 1999, 2000; FTC 1998a, 1998b, 2000a; Hoffman, Novak, and Peralta 1999; Rohm and Milne 1998). Indeed, the U.S. Federal Trade Commission has discussed the potential need for legislation to raise levels of privacy to acceptable standards (FTC 2000), with recent legislative efforts focusing on information disclosure in the form of Web site privacy policies (Miyazaki and Fernandez 2000). Unfortunately, such a focus may be misdirected since privacy policies are not contracts and are subject to change at the discretion of the firm and without notice to the consumer. For example,

Amazon.com recently underwent a widely publicized modification of their privacy policy declaring that the company could trade personal data with other companies, without the need for customer notification (CNN 2000).

Firms with an Internet presence agree that privacy is a key factor for online success. This was illustrated in a recent survey of Internet marketers, wherein fewer than half (46%) of those surveyed felt that Web site self-regulation adequately protects consumers, while 92% believed that consumers would make more online purchases if they felt more confident regarding online privacy (Jarvis 2000). The same survey suggested that a single privacy standard is key to consumer confidence, but that government involvement would harm e-commerce. Congruent with this perspective, a number of companies with an online presence are trying to counter attempts to legislate privacy policies by promoting the value of third-party seals of approval or verification systems designed to temper consumer privacy concerns (Benassi 1999; *Industry Standard* 1999; Palmer, Bailey, and Faraj 2000). The efficacy of these Internet seals of approval, however, has been questioned by the FTC because of both a lack of adoption by online firms and the failure of seal of approval programs to impact privacy practices. For example, a recent FTC (2000) study found that only 8% of heavily-trafficked Web sites it surveyed displayed a seal, and almost one-half of sites displaying seals from popular self-regulated seal programs did not meet the standards set for fair information practices (FTC 2000). This is not surprising considering limitations in the enforcing ability of these programs (Caudill and Murphy 2000).

This situation raises questions as to whether Internet seals of approval are effective in (1) raising online firms' privacy-related practices to acceptable levels and (2) influencing consumers' perceptions of such privacy practices. To address these questions, we present the findings of four studies. The first study examines the state of Internet seals of approval in the

current marketplace. The second study assesses whether firm participation in an Internet seal program is a valid indicator of privacy standards. The final two studies evaluate whether the display of Internet seal of approval logos influences consumer judgments of online firms' privacy efforts. We conclude by discussing the policy implications of the findings. But first, we briefly review prior work concerning seals of approval.

A BRIEF REVIEW OF SEALS OF APPROVAL

Although seals of approval have existed for decades and have been sponsored by a variety of organizations (e.g. Good Housekeeping, American Dental Association, United Laboratories), such seals have received surprisingly little attention in the marketing and consumer behavior literatures. A notable exception is Bennett and McCrohan (1993) who provide a conceptual overview of seals in the food industry. They claim that seals of approval, in theory, may be useful for communicating a threshold of quality to otherwise unknowledgeable consumers, but in practice, may not be in the best interests of consumers. Specifically, Bennett and McCrohan (1993) suggest that the practice of many seal-granting organizations to use such seals as a means to raise revenue may be seen by some consumers and consumer advocates to harm perceptions of impartiality in awarding approval to member firms. Notwithstanding the important issues raised by Bennett and McCrohan (1993), a number of seals of approval continue to be used in today's marketplace.

It may be argued that the potential need for seals of approval is even greater in the context of the Internet. For example, prior research suggests that consumers perceive a great deal of risk with respect to e-commerce when compared to transactions made at traditional brick and mortar outlets (FTC 1998a; Miyazaki and Fernandez 2001; Rohm and Milne 1998; Sheehan and Hoy 2000). This likely occurs due to several features of online transactions, such as the temporal

separation of payment and product delivery, the necessity to provide personal information (e.g., name, address, telephone number) and payment information (e.g. credit card number), and the inability to examine products before making the purchase (Miyazaki and Fernandez 2001). Indeed, while other remote purchasing methods (such as telephone and mail-order shopping) have been shown to elicit relatively high feelings of consumer risk (Cox and Rich 1964; Spence, Engel, and Blackwell 1970), e-commerce likely suffers even further due to its relatively innovative nature and considerable media coverage of security- and privacy-related problems. In addition, problems with online retailer logistics, such as toysrus.com's notification in late December 1999 that holiday orders could not be delivered on time, likely have exacerbated concerns regarding product delivery.

In the context of online transactions and privacy concerns, firms can attempt to reduce consumers' perceived risk in several ways (Hoffman et al. 1999; Machrone 1998), one of which is the use of seals of approval from trusted third parties (Palmer et al. 2000; Krishnamurthy 2001). Such third parties can attest to the particular privacy level that a particular online firm is providing. Consumers who see the seal can then be assured that a certain standard of privacy will be met. Finally, a seal of approval can be thought of as a co-branding strategy (Grossman 1997; Park, Yun, Shocker 1996), wherein a Web site aligns with a trusted third party in an attempt to gain the trust and/or confidence of potential customers (Krishnamurthy 2001).

The strategic design of such seal programs is a key ingredient of their effectiveness. For example, consider the two types of monitoring costs borne by a firm that sponsors and administers a seal program. First, the sponsoring firm must ensure that all members meet the specified requirements to obtain the seal. Second, the sponsoring firm that runs the program must ensure that all members continue to abide by its policies over time. The greater the

requirements (i.e., the more rigorous the program), the higher the costs per member (both initial approval costs and ongoing monitoring costs).

Essentially, this is a one-principal (the sponsoring firm), several-agents (i.e., member firms) problem (cf. Bergen, Dutta, and Walker 1992). Each member realizes that it can benefit by associating with the program. However, some members may not be willing to follow the rigorous requirements of the program, particularly if it is determined that the probability of being discovered and disciplined is relatively low. At the same time, the sponsoring firm, realizing that its credibility is at least partially linked to the number of participating members, may be tempted to allocate resources toward attracting new members rather than toward monitoring current members. The result is a program where low monitoring leads to inconsistent application of the seal of approval and thus, diminished potency and validity.

STUDY 1: INTERNET SEALS IN THE MARKETPLACE

Although several Internet seal of approval programs exist in various forms, the majority of firms involved in such programs currently participate in one or both of the two dominant programs: TRUSTe and BBBOnline (Palmer et al. 2000). TRUSTe and BBBOnline have, respectively, almost 2,000 and 700 participants in their privacy seal of approval programs at the time of writing (TRUSTe 2000b; BBBOnline 2000a). An examination of the top 500 Internet consumer Web sites¹ found that 23.9% of those sites had some form of seal-like emblem, symbol, or endorsement. The examination confirmed that the highest rates of participation in

¹ Top 500 Web sites were based on the Media Metrix 500 (mediamatrix.com), which include commercial online services, Internet service providers, e-commerce, and other ad supported sites based on the most unique visitors (i.e., multiple visits by the same person count only once) over the course of one month (July 2000 for this examination). The list does not include consolidations or networks.

seal of approval programs for this group were for TRUSTe (19.3%) and BBBOnline (4.1%), followed by CPA WebTrust (1.85%), Certified Merchant Guarantee (0.82%), and several others (all with less than 0.5% participation).

Firms willing to participate in the TRUSTe and BBBOnline programs are required to prepare a privacy policy and agree to abide by certain criteria regarding the collection and use of private consumer information. For example, TRUSTe requires licensees to disclose the following information in their privacy statements:

- The personal information gathered by the licensee site.
- The organization collecting such information.
- How the information will be used.
- The choices available to users regarding collection, use, and distribution of information, including opportunities to opt-out of internal secondary uses as well as third-party distribution for secondary uses.
- Security procedures used to protect collected information from loss, misuse, or alteration.
- How users can update or correct inaccuracies in their pertinent information.

A key feature of Internet seals of approval programs is that companies that agree to abide by the seal of approval standards (and pay a registration fee) are authorized to place “privacy seal of approval” logos on their Web sites. Both TRUSTe and BBBOnline contend that consumers who view these logos will then be assured that these companies have been audited for their privacy practices and will feel confident about the privacy of personal information (BBBOnline 2000a; TRUSTe 2000a). Thus, a key factor of seal of approval participation for a firm is the prominent display of the seal of approval logo. Considering the importance of the seal of approval logo in communicating seal program participation, Study 1 was conducted as an exploratory examination of the TRUSTe and BBBOnline programs with respect to who the licensees are and the degree to which the licensees comply with each seal’s logo usage guidelines.

Study 1 Methodology

The lists of TRUSTe and BBBOnline licensees were acquired from each seal's Web site. On both lists were a number of Web sites owned by parent companies using the same privacy page for their product divisions. Because TRUSTe and BBBOnline often list the divisional Web sites as separate licensees, listings which were duplicates of parent company sites were eliminated from the data set.

Using the refined list of licensees, trained researchers visited each licensee Web site to determine firm type, logo type, and logo position. Licensee firms were classified as either domestic or international (from the perspective of the United States since both seal programs are based in the U.S.) using the incorporation address for each firm (obtained from whois.net). Licensee lists also were compared to several "top-firm" lists—the Fortune E-50 (fortune.com), the Fortune 500 (fortune.com), and the Information Week top 100 innovative high-tech companies (informationweek.com)—to examine the reach of the two seal programs.

Study 1 Results

After eliminating duplicate Web sites, the combined (TRUSTe and BBBOnline) licensee list totaled 1,657 firms. Of those 1,657 licensees, 330 firms were registered with BBBOnline, 1,253 with TRUSTe, and 74 with both seal organizations. Although these numbers are negligible when viewed in the context of over 1 billion Web pages worldwide (google.com), the reach of these seals appears to be relatively broad. For example, TRUSTe reports that almost 90% of Internet users will visit a TRUSTe licensed site in any given month (TRUSTe 2000a).

Firm type. Researchers assigned each licensee site to a firm type category based on the information on the particular firm's Web site. Three firm-type categories—online retailers

(44%), Internet portals (19%), and business-to-business firms (11%)—comprised the majority of the licensees. Other firm types were educational (5%), advertising and promotion (4%), news (2%), community (1%), and nonprofit (1%), with the remaining firms not clearly fitting into any of these classifications. The vast majority of licensees (almost 93%) were incorporated within the United States. TRUSTe and BBBOnLine were essentially identical in this respect.

Logo type and location. Both TRUSTe and BBBOnLine require each licensee Web site to post a seal logo that acts as a hyperlink to the seal's site to act as an authentication procedure for visitors to the licensee site. Each licensee site was examined to determine if it displayed a seal logo or words promoting participation in the seal program, and whether either of these was hyperlinked to the appropriate seal site. Only 37% of TRUSTe licensees and 48% of BBBOnLine licensees were found to be in compliance with the required display of a hyperlinked logo. Indeed, almost 12% of TRUSTe licensees and 9% of BBBOnLine licensees did not display any logo at all. Finally, almost 5% of TRUSTe licensees and 8% of BBBOnLine licensees did not have active Web sites.

The location of the seal logo(s) or other seal information on the licensee Web sites was also determined. The majority of licensees (54%) displayed their privacy seal of approval information on both the home and privacy pages of their Web sites. An additional 20% displayed privacy seal information on only a privacy policy page, while another 9% displayed only on the home page.

Top e-company lists. Comparisons against accepted lists of “top” companies showed that 32% of all Fortune E-50 firms, nearly 5% of Fortune 500 firms, and 14% of Information Week 100 firms are TRUSTe or BBBOnLine licensees. TRUSTe accounted for the majority of the licensees, with 26%, 3%, and 10%, respectively, versus BBBOnLine's 8%, 2%, and 4%.

Study 1 Discussion

This examination of the online marketplace demonstrates that Internet seals of approval are fairly limited in their reach with respect to (1) the number of online participants, (2) the geographic location of participating firms, and (3) the types of online firms represented. Indeed, even among top e-commerce firms (such as those in the Fortune E-50 and the Information Week 100), participation in seal of approval programs is quite limited.

In addition, simple required practices such as logo placement and proper logo usage are not consistent across participating firms. This is potentially problematic for online shoppers who are unable to rely on a uniform seal logo display procedure.

Both TRUSTe and BBBOnline claim that a key benefit of enrolling in their seal programs is the added confidence a potential consumer will feel when viewing the seal of approval logo on a licensee Web site. This claim raises two related questions. First, do Web sites that participate in seal of approval programs have “better” privacy policies than comparable Web sites that do not participate? Second, does the presence of a seal of approval logo influence consumer perceptions regarding online privacy? The following three studies were designed to address these questions.

STUDY 2: INTERNET SEALS AND ONLINE PRIVACY POLICIES

The current FTC online privacy standard is based on the Fair Information Practice Principles (FTC 1998 *Privacy Online: A Report to Congress*) that were developed prior to the widespread development of the Internet (HEW 1973). As reported by the FTC (2000), these four principles are:

- Notice: Data collectors must disclose their information practices before collecting personal information from consumers;
- Choice: Consumers must be given options with respect to (1) whether and (2) how personal information collected from them may be used for purposes beyond those for which the information was provided;
- Access: Consumers should be able to view and contest the accuracy and completeness of data collected about them; and
- Security: Data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

Sheehan and Hoy (2000) note that the FTC has declared “notice” as the most fundamental of its fair information practice principles,² with this notice most often being in the form of online privacy policies (Miyazaki and Fernandez 2000). Proponents of Internet seals of approval suggest that privacy-related seals should, as a proposed form of self-regulation for the online industry, result in higher levels of privacy compliance than if no such seals existed. Indeed, TRUSTe and BBBOnline marketing efforts to commercial Web sites imply that the presence of a seal logo on a licensee Web page will demonstrate to online shoppers that the licensee has agreed to operate at a “higher” standard than non-licensee Web sites. This higher performance level could occur for two reasons. First, Web sites that already have relatively high standards of privacy practices can join and benefit from Internet seal of approval programs without the need to make large changes in privacy policies (similarly, Web sites that have relatively low standards of privacy practices would be required to make significant changes in privacy policies if attempting to join and benefit from seal of approval programs, and thus, might be expected to shy away from participation in such programs). Second, Web sites registering with Internet seals of approval

² Although we agree with the Sheehan and Hoy (2000) perspective that “exchange” (i.e., some form of compensation or incentive in exchange for personal information) and seller-buyer relationships likely play key roles in consumers’ perceptions of online privacy, we limit our investigation to the principles currently endorsed by the FTC.

may be motivated to raise privacy-related performance at least to the threshold required by the seal of approval organization. In that several of the seal of approval requirements are similar to FTC privacy guidelines, the following hypothesis can be proposed:

H1a: Web sites that participate in Internet seal of approval programs will have *higher* levels of compliance with the FTC Fair Information Practice Principles than Web sites that do not participate in such programs.

In contrast, concerns have been voiced by the FTC that Internet seals of approval may have little or no effect on online privacy practices from both aggregate and individual Web site perspectives (FTC 2000). This concern may have been fueled by criticism targeted at TRUSTe for not aggressively pursuing some perceived violations of privacy policies.

H1b: Web sites that participate in Internet seal of approval programs will have levels of compliance with the FTC Fair Information Practice Principles that are *no different* than Web sites that do not participate in such programs.

The lack of participation by many popular online firms (e.g., Amazon.com, Buy.com, Travelocity, Ameritrade) may lead consumers to believe that only those firms with a need to externally validate their privacy practices will participate in Internet seal programs. This would imply that licensees may actually have worse online privacy practices than non-licensees, suggesting another competing hypothesis:

H1c: Web sites that participate in Internet seal of approval programs will have *lower* levels of compliance with the FTC Fair Information Practice Principles than Web sites that do not participate in such programs.

Study 2 Methods

Sixty Web sites were chosen from the top 1,000 commercial sites (with respect to traffic) using a stratified random sampling procedure.³ First, the top sites were divided into three groups: sites with no Internet seal of approval participation, sites registered with only the TRUSTe seal, and sites registered with only the BBBOnline seal. Sites with other seals or multiple seals were discarded and were not included in the sampling procedure. Each of the three groups was then randomly sampled for 20 sites. Average traffic (based on aggregated traffic over a one-month period compiled by alexaresearch.com) for each set of 20 sites was similar ($F = 1.22, p = .31$).

The privacy policy information for each site was then printed and individually evaluated by each of three trained judges who were not aware of the research hypotheses. Each privacy policy was evaluated in consideration of the FTC Fair Information Practice Principles described above. First, the Content Analysis Form (questions 9 through 23 which apply to Web site privacy policy compliance) from the FTC (2000) Online Privacy Survey was used to evaluate each privacy policy. Then, seven measurement items (presented in Appendix 1) were developed based on the four principles of notice (disclosure), choice (opt in and opt out), access (and ability to contest accuracy of data), and security (data accuracy and security from unauthorized use). (These items were pretested and found to distinguish between privacy policies that varied in their compliance with the FTC principles.) Judges assessed how well each privacy policy conformed with each statement on a 7-point Likert-type scale anchored with “poor” and “excellent.”

Study 2 Results

The percentage agreement (where all 3 judges corresponded in their responses) for each of the FTC (2000) Online Privacy Survey items for all of the privacy policies examined, ranged from 88.3% to 98.3%, with an average of 92.7% agreement overall. Discrepancies were resolved using a fourth trained judge who was not aware of the research hypotheses.

To test H1, a series of chi-square tests were used to examine for differences across seal conditions (i.e., the TRUSTe seal, the BBBOnline seal, and no seal) with respect to the FTC Online Privacy Survey items. No statistically significant differences were found ($\chi^2_{df=2}$ values ranged from 0.13 to 2.42; all $ps \geq .30$). To examine the seven privacy policy evaluation statements, a series of one-way analyses of variance, using seal of approval (i.e., no seal, TRUSTe, or BBBOnline) as the independent variable and each privacy policy evaluation statement as the dependent variable were conducted. No significant differences were found between seal conditions (all $Fs < 1.69$, all $ps \geq .20$). Thus, there was no support that participation in a seal program is an indicator of privacy practice standards.

Study 2 Discussion

Consistent with FTC concerns, participation in seal programs did not appear to have any influence on individual privacy policy compliance.⁴ This creates a potential policy issue in that many consumers may come to expect that a Web site's participation in a privacy seal of approval program is indicative of a higher standard than nonparticipants. In that there appears to be no

³ A list of top sites was obtained from alexa.com for July 2000.

⁴ This is not to say that Internet seal of approval programs have had no aggregate influence. It is possible that both participating and nonparticipating online firms are motivated to raise their privacy practices to a higher standard due to the presence of seal of approval programs in the marketplace. However, the lack of compliance with FTC guidelines would suggest that any such effects are still lacking.

difference (at least among highly trafficked Web sites), such consumers would be unintentionally misled. In the following two studies, we examine whether consumers perceive differences between Web sites that display seal of approval logos and those that do not.

STUDIES 3 AND 4: INTERNET SEALS AND CONSUMER PERCEPTIONS

In relatively high risk consumption situations, trusted third party endorsements are useful in alleviating consumer concerns. As consumers move from physical to Internet shopping environments, the role of trust becomes increasingly important (Bailey and Bakos 1997). As such, the use of trusted third parties, such as Internet seals of approval, become more beneficial for reducing information disclosure concerns associated with relatively high levels of risk (Palmer et al. 2000). Thus, the Internet seal of approval takes on two roles. First, it serves to inform consumers that the licensee Web site has met some standard with respect to privacy practices, or at the very least the site is concerned about privacy issues. Second, the seal may serve to encourage information disclosure and online patronage by reducing the risks associated with a particular Web site. The first role is fairly straightforward and is presented as the following hypothesis:

- H2: The presence of an Internet seal of approval logo will result in more favorable consumer perceptions regarding the licensee Web site's privacy practices (as opposed to the absence of the seal logo).

The second role, that of encouraging information disclosure and Web site patronage, is likely dependent on the degree to which a consumer experiences concerns regarding online shopping. In that risk perceptions toward online shopping have been shown to be negatively related to online purchase rates (Miyazaki and Fernandez 2001), it follows that consumers experiencing relatively high levels of risk regarding online shopping will be reluctant to disclose

information (e.g., name, address, phone number, etc.) leading toward an online transaction. The use of an Internet seal of approval as a trusted third party should act to reduce online concerns for the licensee and thus encourage information disclosure and online patronage. For consumers with relatively low levels of risk regarding online shopping, the Internet seal of approval will offer no incentive to elevate levels of information disclosure or patronage intentions. Thus, a moderating hypothesis is proposed:

H3: The presence of an Internet seal of approval logo will result in higher levels of information disclosure and anticipated Web site patronage for consumers who experience relatively high levels of online shopping risk; there will be no (or decreased) logo effects for consumers experiencing relatively low levels of online shopping risk.

Two between-subjects experimental studies were designed to test Hypotheses 2 and 3. Study 3 utilized six actual Web site privacy policies that were participants in the various seal programs, while Study 4 manipulated the presence or absence of a seal logo in a more controlled experiment.

Study 3 Methods

A 3 (seal of approval logo) \times 2 (risk toward online shopping) between subjects experiment was designed with the seals of approval (TRUSTe, BBBOnline, or no seal logo) being manipulated, and online shopper risk being measured (and split at the median). Six average-rated Web site privacy policies from Study 2 (two from each seal condition) were chosen on the basis of approximate equality regarding their privacy practice compliance scores. (Since perfect equality could not be achieved with the given set of Web sites, the “no seal” policies had slightly higher compliance scores, a condition that operates counter to the hypotheses and results

in a more conservative test.) The privacy policy pages and home pages were printed in color for each Web site.

After assuring that each subject had regular access to the Internet (either through home or work), he or she was given the printed information from one of the six Web sites and instructed to read the material as if considering conducting business with the online operation. Subjects then responded to several items designed to assess Hypotheses 2 and 3, along with items assessing demographics and Internet usage.

Four items assessed the perceived favorableness of the company's privacy practices (these are shown in Appendix 2). Six items assessed anticipated information disclosure practices by assessing (under the scenario that the subject was "interested in conducting business with this organization and after having an opportunity to examine this organization's privacy policy") the likelihood that the subject would disclose his or her name, personal email address, personal mailing address, personal telephone number, credit card number, and social security number. One 7-point scale item assessed anticipated patronage by asking, "if the organization had a product you desired at a price, including shipping, that was attractive, would you order it?" anchored by "very unlikely to order" and "very likely to order." General feelings of risk toward online shopping were assessed using a 3-item pretested scale (shown in Appendix 2). Demographic and Internet usage measures were also administered.

Study 3 Results

Experimental materials were administered to 204 subjects who were enrolled in various evening or weekend academic programs designed for full-time employees. The use of a nonprobability sample is appropriate in light of the theory-testing aspect of this study, rather than

an attempt to determine average or typical Web usage. Subject ages ranged from 21 to 51, with a mean of 32.9 (median 33). Almost 62% were male with 38% female. Duration of regular Internet access ranged from one month to slightly over eight years, with a mean of 3.4 years (median 3). Monthly usage ranged from 3 to 30 days per month, with a mean of 19.1 days (median 20).

The three risk items were combined (standardized $\alpha = .91$) to form an overall risk toward online shopping score. This was split at the median (4.3) to create low and high conditions. The four items assessing perceived favorableness of the privacy policy were also combined (standardized $\alpha = .90$). Hypothesis 2 was tested using a 2-factor ANOVA model with seal of approval (3 levels) as one factor, the median-split risk score as the second factor, and the privacy policy favorableness measure as the dependent variable. The overall model was significant ($F=17.7, p<.01$) with the seal factor having the expected impact on privacy policy favorableness ($F=43.8, p<.01$) and risk having no effect ($F=.03, n.s.$). Planned contrasts showed both the TRUSTe ($M=5.3$) and BBBOnLine ($M=5.7$) seals to be higher than the no seal condition ($M=4.0$; both $ps<.05$), with no differences between the two seal-present conditions. The results were the same across both high and low online risk conditions.

Hypothesis 3 was tested using a series of two-factor ANOVA models, with the dependent variables for each being the information disclosure items and the anticipated patronage item. As presented in Table 1, the 2-way interaction was significant (all $ps<.05$) for all the disclosure items except for social security number. As hypothesized, planned contrasts showed the two seal conditions to have higher anticipated disclosure rates (except for social security number) than the no seal condition when online shopping risk was high (all $ps<.05$), but not when online shopping risk was low (all $ps>.27$). Anticipated patronage operated similarly, with the significant

interaction ($F=3.5, p<.05$) showing the presence of a seal of approval to result in higher anticipated patronage under high risk conditions ($F=14.3, p<.01$), but not under low risk conditions ($F=1.7, p=.18$). Means and statistics are shown in Table 1.

Study 3 Discussion

The results from Study 3 provide evidence that a seal of approval can influence consumer perceptions of favorableness toward a Web site privacy policy. In addition, the seals can affect anticipated information disclosure and site patronage for high risk consumers, but not for low risk consumers.

Although the privacy policies evaluated in Study 3 were rated similarly (in Study 2) with respect to compliance with FTC guidelines, the study is limited in that identical policies were not used in each condition. Thus, differences in consumer perceptions may be attributed to differences in the privacy policies (although all were rated similarly in Study 2) rather than the presence of an Internet seal of approval. Study 4 remedies this limitation by using a more controlled set of stimuli to extend the results of Study 3.

Study 4 Methods

The Study 4 experimental design was identical to Study 3 except that the privacy policy was identical across seal of approval conditions, and the seal manipulation consisted of one seal absent condition and one seal present condition (using the BBBOnLine logo placed at the top right on the privacy policy page). The other difference was that only the privacy policy was viewed and it was viewed on a computer screen rather than in printed form.

Study 4 Results

Experimental materials were administered to 35 subjects who enrolled in a weekend academic program designed for full-time employees. Subject ages ranged from 24 to 52, with a mean of 34.4 (median 33). Almost 66% were male with 34% female. Duration of regular Internet access ranged from three months to seven years, with a mean of 3.4 years (median 3.1). Monthly usage ranged from 3 to 30 days per month, with a mean of 22.5 days (median 24).

As in Study 3, risk toward online shopping (standardized $\alpha = .93$) was split at the median to create low and high conditions. Hypothesis 2 was tested using a 2-factor ANOVA model with seal of approval (logo present or absent) as one factor, the median-split risk score as the second factor, and the privacy policy favorableness measure (standardized $\alpha = .93$) as the dependent variable. The overall model was significant ($F=11.6, p<.01$), with the logo present condition resulting in higher privacy policy favorableness ($M=5.14$) than the logo absent condition ($M=3.51; F=33.9, p<.01$). Risk toward online shopping had no effect; the logo effects were the same across both high and low online risk conditions.

Hypothesis 3 was tested using a series of two-factor ANOVA models, with the dependent variables for each being the information disclosure items and the anticipated patronage item. Although the interaction term did not reach statistical significance in the ANOVA models, planned contrasts showed that the presence of the seal logo had no effect for consumers with relatively low levels of online shopping risk, but did have an effect for consumers with higher online shopping risk. As presented in Table 2, this effect was present for anticipated disclosure of name, email, and mailing address (all $ps < .05$), but not for phone, credit card, or social security number. The effect was also present for anticipated patronage ($p < .05$).

Study 4 Discussion

The results for Study 4 corroborate those of Study 3, and with a more controlled set of experimental stimuli, although using a smaller sample size that resulted in less statistical power. In sum, the presence of the Internet seal of approval logo was shown to raise consumer perceptions of a firm's privacy-related practices, regardless of the consumer's level of online shopping risk. However, the presence of the logo only affected anticipated information disclosure and patronage decisions for consumers with higher levels of online shopping risk, and not for those with lower levels.

GENERAL DISCUSSION

Although Internet seals of approval have been proposed as a non-legislative method of ensuring online privacy standards, concerns raised by the Federal Trade Commission and consumer advocacy groups have suggested that the efficacy of such seals is limited. A series of studies was conducted to examine the state of Internet seals of approval and their impact on e-commerce. Study 1 found that licensee compliance with even simple seal of approval program requirements such as seal logo use and placement is not high, and that the reach of such programs is limited. Study 2 suggested that participation in seal programs has no bearing on the online privacy practices of firms as reflected in their Web site privacy policies. However, Studies 3 and 4 showed that the mere display of an Internet seal of approval logo enhances consumer perceptions regarding privacy policy favorableness. Furthermore, as expected, the presence of seal logos were found to increase anticipated disclosure and patronage rates for consumers with relatively high online shopping risks, but had no effects on consumers with low online shopping risks.

Implications for Online Firms and for Public Policy

The main implications of this research are the contrasts between Study 2 and Studies 3 and 4. Specifically, consumers are likely to believe that a site maintains a higher privacy standard when that site participates in an Internet seal of approval program, although they are unlikely to find any objective differences in privacy policies among firms that exhibit a seal and those that do not. Hence, the higher standard of privacy practice perceived by consumers due to the presence of a seal of approval may be unwarranted. This suggests that legislation specifically requiring firms to follow the FTC fair information practices may be more effective in establishing appropriate privacy practice standards than the current Internet seal of approval programs, as alluded to in FTC (2000). Any legislation would need to consider more recent research on Internet privacy; for example, Sheehan and Hoy (2000) suggest that the inclusion of factors beyond the FTC's four privacy principles, such as consumer expectations of fair exchange, would lead to a more complete set of online privacy standards (see also Culnan and Armstrong 1999).

A positive aspect of the findings for Internet seal of approval programs is that participation in the seal programs studied here do appear to have a favorable effect on consumer perceptions. This is good news for online firms that are concerned whether membership in seal programs and display of seal logos are effective in reducing privacy concerns for potential and current consumers (Palmer et al. 2000). These firms would prefer that consumers recognize such seals as a symbol of trust, insurance, etc. with respect to online privacy. However, these goals would be difficult to accomplish if participation by licensees is inconsistent and seal program sponsors do not regulate licensees as promised. Indeed, there have been concerns that programs funded by for-profit corporations may not be aggressive in pursuing any privacy infractions

among revenue-generating licensees. For example, one of the seal programs examined here, TRUSTe, was criticized for being too lenient on seal licensees RealNetworks and Microsoft, although more recently it has become more aggressive in its enforcement of privacy standards, such as in its filing against Toysmart's attempt to sell its customer database (*The Standard* 2000).

The current set of studies also reveals a bias toward U.S. firms as licensee members of the seals examined here. This is a concern considering the global nature of the Internet which is so widely touted in the media as one of e-commerce's most beneficial features. Positive steps are being taken by at least one of the seal programs in that TRUSTe has now established a specific international program (TRUSTe 2000b).

If Internet seal of approval programs are to continue, there appear to be several issues that must be considered if such programs are to be successful. First, as noted previously, seal of approval programs must have sufficient resources to cover both initial approval costs and ongoing monitoring costs. Clearly, these costs can be reflected in periodic registration fees. However, the potential for such fees to escalate to unreasonably high levels could exclude participation from smaller companies that may otherwise qualify for seal program participation.

Another concern is that if seal programs are having difficulty in governing their relatively small numbers of licensee firms, it seems unlikely that such programs could accommodate the type of substantial growth common to e-commerce. Indeed, if such seal programs were to fail to remain effective as their member base grows, it would appear likely that government intervention would be necessary.

Limitations and Future Research

There are several limitations to the current set of studies that should be addressed in future research. First, there is the issue of timeliness that is typically raised when considering

empirical research on e-commerce. While we agree that Study 1 is limited in its ability to reflect an up-to-the-minute view of the seal of approval marketplace, it is a thorough examination of the state of online seals and is necessary to provide a relatively current understanding of that marketplace (that could be updated as needed). If seal of approval programs begin to experience substantial growth, it might be useful to monitor not only the nature of their membership and reach, but also their impact as done here in Studies 2, 3, and 4.

Study 2's evaluation of privacy policies provided reasonable evidence of the ineffectiveness of seal of approval programs to offer consumers a valid cue for delineating various levels of privacy practices, at least with respect to privacy policies. Although a much more daunting task, future research might go beyond an examination of privacy policies and attempt to assess actual privacy practices. Perhaps it is in firms' actions, and not just in their privacy policies, that differences between seal participants and nonparticipants will become evident.

Finally, Studies 3 and 4 are limited in that they did not utilize natural shopping environments. In their defense, however, it would be expected that in a natural setting (with more distractions and less focus on the privacy policy stimuli), consumers would have less intensive processing of privacy policy content and thus even more need to rely on cues to favorable privacy practices such as seal of approval logos. Thus, Studies 3 and 4 likely represent conservative tests of whether seal logos act as cues to consumers. Furthermore, the potential for demand artifacts is small if even present considering that (1) no subjects stated any awareness of the research hypotheses in the demand artifact item and (2) the moderator hypothesis (H3) was supported in two between-subjects experiments, with this type of hypothesis being much less likely to suffer from demand artifacts than simple main effects hypotheses.

Nevertheless, future research should continue to investigate what factors affect consumer perceptions of their privacy with online firms. While prior work has touched upon the importance of seals of approval in influencing trust (e.g., Palmer et al. 2000), most examinations of consumer online privacy perceptions have noticeably excluded the impact of seals. In addition, the findings that online risk perceptions moderate the influence of seal participation on disclosure and anticipated patronage suggests that individual risk should continue to be a primary consideration when studying consumers' privacy perceptions. Finally, prior work regarding consumer trust (e.g., Milne and Boza 1999; Morgan and Hunt 1994) suggests that research examining the role that trust plays in the perception of Internet seals of approval will shed much light on their effectiveness in reducing risk.

REFERENCES

- Bailey, Joseph P. and Yannis Bakos (1997), "An Exploratory Study of the Emerging Role of Electronic Intermediaries," *International Journal of Electronic Commerce*, 1 (Spring), 7-20.
- Benassi, Paola (1999), "TRUSTe: An Online Privacy Seal Program," *Communications of the ACM*, 42 (February), 56-59.
- Bennett, James T and Kevin F. McCrohan (1993), "Public Policy Issues in the Marketing of Seals of Approval for Food," *Journal of Consumer Affairs*, 27 (2), 397-415.
- Bergen, Mark, Shantanu Dutta, and Orville C. Walker, Jr. (1992), "Agency Relationships in Marketing: A Review of the Implications and Applications of Agency and Related Theories," *Journal of Marketing*, 56 (July), 1-24.
- BBBOnline (2000a), Homepage <http://www.bbbonline.org> accessed November 2, 2000.
- Boulding, William and Amna Kirmani (1993), "A Consumer-Side Experimental Examination of Signaling Theory: Do Consumers Perceive Warranties as Signals of Quality?" *Journal of Consumer Research*, 20 (June), 111-123.
- Caudill, Eve M. and Patrick E. Murphy (2000), "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing*, 19 (Spring), 7-19.
- CNN (2000), "Analysis: Who Cares About Amazon.com's Privacy Policy?" <http://www.cnn.com/2000/TECH/computing/10/02/amazon.privacy.idg/index.html> (October 2).
- Cox, D.F. and S.U. Rich (1964), "Perceived Risk and Consumer Decision Making—The Case of Telephone Shopping," *Journal of Marketing Research*, 1, 32-39.
- Culnan, Mary J. (1999), "Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission," (June), <http://www.msb.edu/faculty/culnanm/gippshome.html> accessed July 27, 1999.
- Culnan, Mary J. (2000), "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing*, 19 (Spring), 20-26.
- Culnan, Mary J. and Pamela K. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organizational Science*, 10 (January), 104-115.

- Federal Trade Commission (1998a), "FTC Releases Report on Consumers' Online Privacy," FTC Press Release dated June 4, 1998, FTC File No. 954-4807.
- Federal Trade Commission (1998b), "Consumer Privacy on the World Wide Web," prepared statement presented to the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, United States House of Representatives, July 21, Washington, DC.
- Federal Trade Commission (2000), "Privacy Online: Fair Information Practices in the Electronic Marketplace," Report to Congress, May 2000, available at <http://www.ftc.gov>..... (accessed June 2, 2000).
- Grossman Randi Priluck (1997), "Co-Branding in Advertising : Developing Effective Associations", *Journal of Product and Brand Management*, 6 (3).
- Hoffman, Donna L., Thomas P. Novak, and Marcos Peralta (1999), "Building Consumer Trust Online," *Communications of the ACM*, 42 (April), 80-85.
- Industry Standard, The* (1999), "Ecommerce Spotlight: Building Trust Online," 47 (February 1).
- Jarvis, Steve (2000), "Companies Tell All about Consumer Privacy," *Marketing News*, 34 (December 4), 3.
- Kirmani, Amna (1990), "The Effect of Perceived Advertising Cost on Brand Perceptions," *Journal of Consumer Research*, 17 (September), 160-171.
- Krishnamurthy, Sandeep (2001), "An Empirical Study of the Causal Antecedents of Customer Confidence in E-Tailers," *First Monday*, 6 (January), available at: http://firstmonday.org/issues/issue6_1/krishnamurthy/index.html.
- Milne, George R. and María-Eugenia Boza (1999), "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing*, 13 (1), 5-24.
- Miyazaki, Anthony D. and Ana Fernandez (2000), "Internet Privacy and Security: An Examination of Online Retailers," *Journal of Public Policy & Marketing*, 19 (Spring), 54-61.
- Miyazaki, Anthony D. and Ana Fernandez (2001), "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *Journal of Consumer Affairs*, 35 (1), forthcoming.
- Morgan, Robert M. and Shelby D. Hunt (1994), "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, 58 (July), 20-38.

- Nelson, Phillip (1970), "Information and Consumer Behavior," *Journal of Political Economy*, 78 (March/April), 311-329.
- Palmer, Jonathan W., Joseph P. Bailey, and Samer Faraj (2000), "The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements," *Journal of Computer-Mediated Communication*, 5 (March), available at <http://www.ascusc.org/jcmc/vol5/issue3/palmer.html> (accessed July 3, 2000).
- Park C. Whan, Sung Youl Jun, and Allan D. Shocker (1996), "Composite Branding Alliances: An Investigation of Extension and Feedback Effects," *Journal of Marketing Research*, 33 (November), 453-466.
- Rohm, Andrew J. and George R. Milne (1998), "Emerging Marketing and Policy Issues in Electronic Commerce: Attitudes and Beliefs of Internet Users," in *Marketing and Public Policy Proceedings*, Vol. 8, Alan Andreasen, Alex Simonson, and N. Craig Smith, eds. Chicago: American Marketing Association, 73-79.
- Sheehan, Kim Bartel and Mariea Grubbs Hoy (2000), "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, 19 (Spring), 62-73.
- Spence, Homer, E., James F. Engel, and Roger D. Blackwell (1970), "Perceived Risk in Mail-Order and Retail Store Buying," *Journal of Marketing Research*, 7 (August), 364-369.
- TRUSTe (2000a), "The TRUSTe Story," http://www.truste.com/about/about_truste.html accessed November 2, 2000.
- TRUSTe (2000b), "TRUSTe Unveils European Union Safe Harbor Privacy Seal Program: World's Largest Privacy Certification Program Makes Landmark Move to Provide Global Online and Offline Dispute Resolution," http://www.truste.com/about/about_eu.html accessed November 2, 2000.

TABLE 1
SEAL AND RISK EFFECTS FOR STUDY 3

Disclosure Item	High Online Shopping Risk				Low Online Shopping Risk			
	No Seal	TRUSTe	BBB	<i>F</i>	No Seal	TRUSTe	BBB	<i>F</i>
Name	2.90	4.75	5.19	22.82**	4.97	5.14	5.42	0.91
Email address	2.62	4.47	4.97	24.59**	4.90	5.03	5.44	1.29
Mailing address	1.85	3.63	4.19	24.59**	3.93	4.11	4.53	1.16
Phone number	1.59	2.91	3.59	15.25**	3.10	3.50	3.75	1.26
Credit card #	1.28	2.38	2.94	12.14**	2.72	3.08	3.33	1.22
Social security #	1.13	1.50	1.66	2.77	1.59	1.47	1.72	0.53
Anticipated Patronage	2.56	3.75	4.69	14.24**	4.48	4.75	5.17	1.75

* $p < .05$

** $p < .01$

TABLE 2
SEAL AND RISK EFFECTS FOR STUDY 4

Disclosure Item	High Online Shopping Risk			Low Online Shopping Risk		
	No Seal	BBB	<i>t</i>	No Seal	BBB	<i>t</i>
Name	2.22	4.11	2.81*	4.38	4.56	0.31
Email address	2.22	3.89	2.34*	4.13	4.22	0.14
Mailing address	2.11	3.78	2.17*	3.25	4.00	0.93
Phone number	2.11	2.44	0.68	2.00	2.78	1.34
Credit card #	1.67	2.11	1.05	2.75	3.22	0.57
Social security #	1.22	1.78	1.14	1.00	1.33	1.33
Anticipated Patronage	2.33	3.67	2.31*	3.88	4.33	0.73

* $p < .05$

** $p < .01$

APPENDIX 1
STUDY 2 PRIVACY POLICY EVALUATION SCALE ITEMS

Each FTC Fair Information Practice Principle (FTC 1998 *Privacy Online: A Report to Congress*; 2000a) is followed by the item(s) assessing a firm's compliance with that principle. (Each item was assessed using a 7-point Likert-type scale anchored with "Poor" and "Excellent.")

Notice: Data collectors must disclose their information practices before collecting personal information from consumers.

1. The data collectors disclose their information practices before collecting personal information from consumers.

Choice: Consumers must be given options with respect to (1) whether and (2) how personal information collected from them may be used for purposes beyond those for which the information was provided.

2. Consumers are given options with respect to whether personal information collected from them may be used for purposes beyond those for which the information was provided.
3. Consumers are given options with respect to how personal information collected from them may be used for purposes beyond those for which the information was provided.

Access: Consumers should be able to view and contest the accuracy and completeness of data collected about them.

4. Consumers are able to view the accuracy and completeness of data collected about them.
5. Consumers are able to contest the accuracy and completeness of data collected about them

Security: Data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

6. Data collectors take reasonable steps to assure that information collected from consumers is accurate.
7. Data collectors take reasonable steps to assure that information collected from consumers is secure from unauthorized use.

APPENDIX 2
MEASUREMENT ITEMS USED IN STUDIES 3 AND 4

Four items assessing favorableness toward the company's privacy policy (the fourth was reverse coded):

1. Compared to other organizations with an online presence, how does the organization that displays this policy on its web site view consumer privacy issues?

Not at all serious about consumer privacy	1	2	3	4	5	6	7	Extremely serious about consumer privacy
--	---	---	---	---	---	---	---	---

2. Compared to other organizations with an online presence, how does the organization that displays this policy on its web site view consumer privacy issues?

Not at all dedicated to consumer privacy	1	2	3	4	5	6	7	Extremely dedicated to consumer privacy
---	---	---	---	---	---	---	---	--

3. Compared to other organizations with an online presence, what is the likelihood that the organization that displays this policy on its web site will treat consumers fairly with respect to consumer privacy issues?

Very Unlikely to Treat Consumers Fairly	1	2	3	4	5	6	7	Very Likely to Treat Consumers Fairly
--	---	---	---	---	---	---	---	--

4. Compared to other organizations with an online presence, what is the likelihood that the organization that displays this policy on its web site will violate acceptable privacy standards.

Very Unlikely to Violate Privacy Standards	1	2	3	4	5	6	7	Very Likely to Violate Privacy Standards
---	---	---	---	---	---	---	---	---

Three items assessing general risk toward online shopping (the second and third were reverse coded). Each was accompanied by a 7-point response scales anchored with Strongly Disagree and Strongly Agree.

1. In general, I feel that purchasing products or services over the Internet is risky.
2. I typically feel comfortable using the Internet to purchase goods or services.
3. Purchasing things over the Internet is a safe thing to do.