

## Association for Information Systems AIS Electronic Library (AISeL)

---

AMCIS 2011 Proceedings - All Submissions

---

8-6-2011

# The Effect of Website Quality on Information Disclosure: A Cue Utilization Theory Perspective

Nathan Johnson

*Washington State University, njohnson76@wsu.edu*

John D. Wells

*University of Massachusetts Amherst, jwells@som.umass.edu*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2011\\_submissions](http://aisel.aisnet.org/amcis2011_submissions)

---

### Recommended Citation

Johnson, Nathan and Wells, John D., "The Effect of Website Quality on Information Disclosure: A Cue Utilization Theory Perspective" (2011). *AMCIS 2011 Proceedings - All Submissions*. 409.  
[http://aisel.aisnet.org/amcis2011\\_submissions/409](http://aisel.aisnet.org/amcis2011_submissions/409)

This material is brought to you by AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2011 Proceedings - All Submissions by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# The Effect of Website Quality on Information Disclosure: A Cue Utilization Theory Perspective

**Nathan Johnson**  
Washington State University  
njohnson76@wsu.edu

**John Wells**  
University of Massachusetts  
jwells@som.umass.edu

## ABSTRACT

As shopping through e-commerce portals continues to grow, personal information disclosure is becoming more commonplace. The proposed research employs Cue Utilization Theory (CUT) to better understand how extrinsic cues, intrinsic cues, or a combination of both, influence truthful consumer disclosure of personal demographic information. The two relevant cues used in the study are security features (website seals and security statements) and website visual appeal (VAP). Two studies, a lab experiment and a field study utilizing a snowball sample, will expose subjects to mock-up e-commerce sites that vary high and low components of the cues and present a shopping simulation to determine the cues' influence on truthful disclosure decisions. We posit that VAP will drive stronger predictive and critical values than security features, thereby having greater impact on truthful disclosure. Results from these two studies will be presented at the conference. Contributions and limitations of the proposed research are discussed.

## Keywords

e-commerce, information disclosure, security, visual appeal, cue utilization theory, intrinsic cues, extrinsic cues

## INTRODUCTION

The growth of electronic commerce (e-commerce) has spawned a wide range of online outlets for consumers to purchase goods and services. According to US Census Bureau estimates, e-commerce sales reached \$134.9 billion in 2009. Consumers have witnessed the online store front move beyond simple household items like books and music to expensive commodities such as cars and real estate. As consumer information continues to be catalogued in online databases, more complete shopper profiles can be developed by advertising and marketing firms. In addition, the personal details of consumers are targets for criminal hackers looking to compromise online databases and steal customer data. According to the consumer organization Privacy Rights Clearinghouse, over 353 million records containing personal data have been involved in security breaches since January of 2005 in the US alone (Privacy Rights Clearinghouse 2010). As a result, online security has become a key issue for many consumers utilizing the web.

However, consumers encounter a range of security features in online environments. For example, financial services sites typically employ complex and lengthy security systems to help protect their clients. Customers must use complex usernames, passwords, and work through a set of gatekeeper technologies in order to access site services. Other websites, such as e-commerce sites, usually do not impose the same stringent levels of security measures on customers wanting to use their portals. Still other sites offer up little to no assurance of security to those perusing the page. Research has shown that consumers evaluate the financial reward, their return on information, and improvements of service in future transactions when contemplating personal information disclosure (Goodwin 1991; Milne and Gordon 1993; Sheehan and Hoy 2000). Since consumer disclosure of personal information drives advertisement and marketing efforts, understanding what leads consumers to disclose accurately is vital to industry.

*Cue Utilization Theory* (CUT) is a viable theoretical lens in which to evaluate this dynamic of consumer behavior. The theory's basic tenet is that any entity of interest (a product, service, organization, etc.) is made up of an assortment of cues that denote quality (Olson and Jacoby 1972). In this paper, CUT is applied in an effort to understand a consumer's willingness to truthfully and accurately disclose their information in an e-commerce environment.

The paper is organized as follows. The next section presents a review of the current literature on information disclosure and the e-commerce setting, CUT, website characteristics as cues, and security/non-security related cues. The following section will discuss the research hypotheses and present the research model. Next, the proposed methodology for conducting the

study will be discussed including experiment design and variables. The final section provides discussion of the study, along with expected implications, limitations of the study, and conclusion.

## LITERATURE REVIEW

### Concept of Information Disclosure

The Merriam-Webster dictionary defines the word disclose as exposing to view or making known. In Psychology, self-disclosure is the act of giving personal information to someone else to facilitate a relationship (Jourard 1971; Collins and Miller 1994). The shared information can exist between pairs of people, in groups, or between organizations and the individual (Joinson and Paine 2007). Many avenues of self disclosure research have been completed since Jourard's 1964, 1971) initial studies on the subject. The development of Social Penetration Theory helped to further refine how relationships are developed through a series of self disclosures, progressing from abstract to intimate disclosures (Altman and Taylor 1973). Collins and Miller found that those who provide intimate disclosures are more liked than those who disclose information on a less intimate level. In addition, they found that people disclose more information to those that they like and people like those whom they disclose to (Collins and Miller 1994). An interesting conclusion from a review of self disclosure literature found that when dealing in sensitive personal information, self-disclosure by medical patients increased when they used computerized forms as opposed to face-to-face interviews (Weisband and Kiesler 1996). Similarly, Joinson (2001) found that self-disclosures were significantly higher in computer-mediated communication (CMC) than in face-to-face conversation, and visual anonymity had significant positive effects on the amount self disclosure in CMC sessions.

In the marketing and consumer behavior arena, disclosure is a key concept. Advertisers' promotional campaigns and targeted marketing methods are based on information gathered about consumers (White 2004). Much of this information comes from the mining of personally disclosed consumer information from a variety of sources. Consumers disclose information about themselves and often unknowingly, their habits, in an assortment of ways (Miyazaki and Fernandez 2000). A few examples include the filling out of application forms, government interactions, requesting products or information by mail, website registration, and the use of supermarket club cards. Data collected through these exchanges are stored, aggregated, and often sold to data mining organizations for analysis (Sovern 1999). When consumers knowingly give up their information, research has shown that they are more willing to disclose demographic information rather than information about their financial status or personally identifiable data (Phelps, Nowak, and Ferrell 2000). In their 2007 work, Nordberg and colleagues developed the concept of the privacy paradox. The study's main finding was that consumers' actual levels of disclosure to marketers were higher than their intended level of disclosure (Nordberg, Horne, and Horne 2007). The advent of e-commerce and the massive data storage and retrieval capabilities available to anyone have now brought an unprecedented level of information to marketers' fingertips (Agrawal and Srikant 2000).

### Ecommerce and Information Disclosure

Information disclosures in e-commerce settings have been studied at length. For instance, prior research indicates that computers are able to obtain useful consumer information when they act according to socially approved norms of communication (Moon 2000). Hui, Tan, & Goh (2006) found that consumers can be induced to disclose their personal information to e-commerce sites if they receive certain benefits such as monetary savings, time savings, pleasure, or novelty.

Conti and Sobiesk's (2007) research focused on disclosure and data retention in online environments. Their findings pointed out that online users don't blindly trust that the sites they visit will be good stewards of their personal data. Instead, users believe their privacy on the web is a personal responsibility (Conti and Sobiesk 2007). McKnight, Choudhury, and Kacmar (2002) found trust to be a guiding force when consumers try to overcome perceptions of risk or insecurity in an e-commerce setting. Liu, Lu, and Yu (2005) looked at how an individual's perception of privacy relates to their behavioral intentions to complete an online purchase. Perceptions of privacy had a strong influence on whether or not a potential buyer trusted the e-commerce site, and influenced their intention to purchase or revisit the site (Liu et al. 2005). Metzger's (2006) research noted that a vendor's reputation led to higher consumer trust in their online marketplace, while the consumer's sense of privacy and security did not affect their level of information disclosure to the vendor.

Although online shoppers carry a preconceived set of privacy standards into an e-commerce session, they don't always act according to those standards. A prior study found that shoppers tended to forget about their privacy concerns once they were "inside the Web" (Spiekermann, Grossklags, and Berendt 2001). A follow up research study found that e-commerce shoppers appreciate interactive environments filled with rich content. Once they begin interacting within the site, inhibitions are lowered and they are willing to talk about themselves. This lowering of inhibitions led to a lack of monitoring of what was disclosed, confirming the earlier study that users often forget about their privacy concerns once interaction with the site begins (Berendt, Gunther, and Spiekermann 2005).

**Cue Utilization Theory**

*Cue Utilization Theory* (CUT) is useful when gauging consumers’ perception of quality. According to CUT, products display a range of cues that act as proxies of quality to potential buyers (Cox 1967; Olson 1972). These cues come to light through the associated predictive value (PV) and confidence value (CV) attached to them. PV represents how much consumers equate a product’s quality with the cue, while CV represents how confident consumers are in their ability to judge quality by the cue (Richardson, Dick, and Jain 1994).

Beyond PV and CV, product cues can be further broken down into intrinsic and extrinsic cues (Olson 1972; Olson and Jacoby 1972). Extrinsic cues like price, packaging, or warranty, are related to, but not actually part of, a product itself; intrinsic cues such as the size and placement of buttons on a computer mouse, are part of the makeup of the product and cannot be modified without affecting the product itself (Longstreet 2010; Richardson et al. 1994). Prior research has shown that consumers typically rely more on extrinsic cues rather than intrinsic ones when they are unlikely to devote much thought to the product, have limited time to evaluate it, or when extrinsic cues are more abundant (Chatterjee, Heath, and Mishra 2002; Dawar and Parker 1994; Zeithaml 1988). Although CUT has been leveraged as a method for understanding how consumers perceive products, the present research aims to examine users’ perceptions of e-commerce website cues and how those cues influence their willingness to truthfully disclose information to the site.

*Website Characteristics as Information Cues*

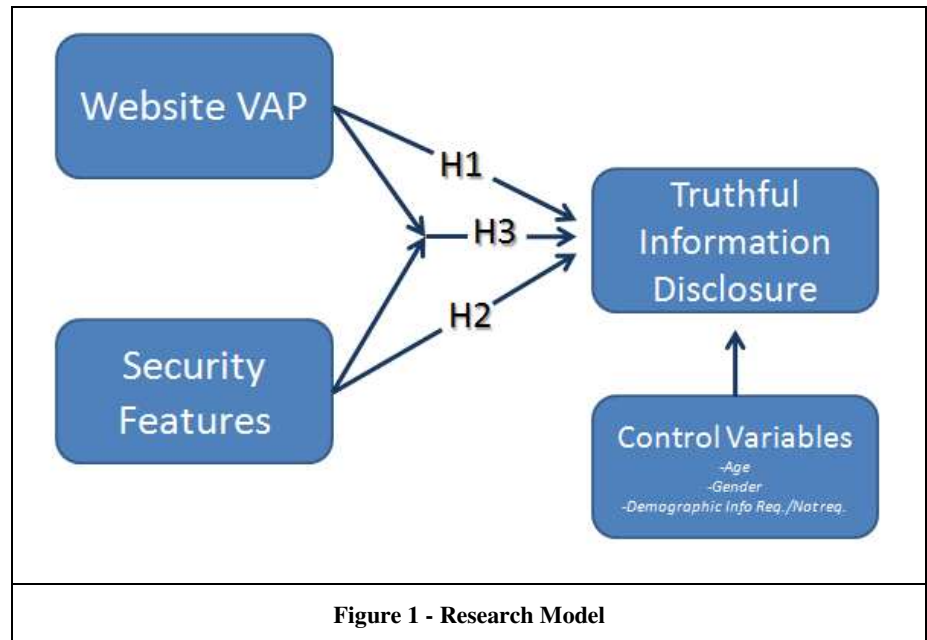
The way an organization’s website is constructed communicates a lot to the visitor. There are two key website characteristics that can be classified as extrinsic and intrinsic cues in e-commerce settings. In this study, the presence of security seals and written security statements (collectively “security features”) concerning privacy of disclosed data will be used as intrinsic cues. A variety of security measures can be employed on a website and described in the security statements such as secure sockets layer encryption, session management, and access time restrictions (Grossman 2008). However, many users will have little knowledge of these methods, and hence a low CV for evaluating them. Likewise, many sites have a plethora of “seals” on them making it more difficult to associate value with any one seal, therefore lowering PV.

The other key website characteristic, visual appeal (VAP), is the extrinsic cue. Much research has gone into determining what gives websites strong VAP (Bucy, Lang, Potter, and Grabe 1999; Cormier 1999; Hoque and Lohse 1999; Lindgaard, Fernandes, Dudek, and Brown 2006; Nielsen 1999; Ranganathan and Ganapathy 2002). In general, sites with strong VAP are pleasing to the eye, easily navigated, share common attributes of other high quality sites, and have competent design. Sites with low VAP have a marked absence of these qualities. VAP is quickly evaluated by users as they begin interacting with the site encouraging PV and CV judgment.

**RESEARCH HYPOTHESES**

In the following section, we present our research hypotheses. Given the two key cues typically found on e-commerce sites discussed earlier, we propose a research model consisting of security features and website VAP as shown in Figure 1.

Website VAP gives users important extrinsic cues for making determinations about a site’s parent organization. In McKnight et al.’s 2002 research, three e-commerce constructs were examined, one of which was website quality. Several items made up the construct such as website technical features, visual likeness with other highly thought of sites, ease of navigation, and how easily information could be located. They found that high-quality websites led consumers to believe that the



**Figure 1 - Research Model**

organization responsible for the site was competent, honest, and kind (McKnight et al. 2002). Prior research has found that by placing professional stock photographs of people on poorly performing vendor's websites, experimental subjects' level of trust in the vendor was raised (Riegelsberger, Sasse, and McCarthy 2003). Website quality has also been found to have a strong positive impact on the initial trusting beliefs of consumers when dealing with unknown brands (Lowry, Vance, Moody, Beckman, and Read 2008). Thus, a well-designed website with high VAP will increase the likelihood of consumers disclosing information to website.

CUT postulates that PV allows consumers to equate quality with a cue, while CV represents how confident consumers are in their ability to judge quality by the cue. Both PV and CV cues act as proxies of quality to consumers. Within moments of reaching a site, consumers can visually make PV and CV judgments about the organization presenting the e-commerce portal. In fact, research has shown that users can make a visual judgment about whether or not they like a web page in 50 milliseconds (Lindgaard et al. 2006). High VAP sites allow rapid PV and CV judgments to be made about the quality of the website and its vendor, thus:

*H1: Website VAP will result in higher consumer CV and PV than Security Features, making it a stronger predictor of truthful disclosure of information over Security Features in e-commerce settings.*

A website's security features are useful intrinsic cues for users that are trying to make judgments about a website's parent organization. Security seals have been shown to raise the level of anticipated disclosure by users that view online shopping as risky. In addition, they have elevated users' perceptions about an organization's privacy practices (Miyazaki and Krishnamurthy 2002). Similarly, Rifon, LaRose, and Choi (2005) found that web seals augment consumer trust in the website in which they are displayed and consumer expectations that the website owner would inform them of their information practices also rose. Written security statements detailing privacy practices and information disclosure policies have also been found to influence trust in website vendors. Hoffman, Novak, and Peralta (1999) found that 69% of web users won't provide their data to websites that don't explain how they will use it. A recent field study reported that the existence of security statements led more study participants to disclose their personal details, although the presence of a privacy seal did not (Hui, Teo, and Lee. 2007). Milne & Culnan (2004) reported that security statements are used as part of an overall strategy by organizations to help manage the risks associated with e-commerce. Results from the study showed users read security statements on websites, especially when they were concerned about control over how their information would be used, unless they were already familiar with the parent organization. Consistent with these findings, we believe that security features on a website should lead consumers to be more willing to disclose their information to the site.

However, from a CUT perspective, security features may not cue the consumer as rapidly as VAP. As noted earlier, due to the technical nature of many security features, consumers are likely to have lower CV. With the abundance legitimate and counterfeit seals (merely the copied image of a security seal) populating the web, PV is likely to be lowered as well, thus:

*H2: Security Features will result in lower consumer CV and PV than Website VAP, making it a weaker predictor of truthful disclosure of information over Website VAP in e-commerce settings.*

Where VAP cues allow a user to make a judgment call from the mere presence (or lack of) certain qualities, security features require more cognitive engagement by the user in order to form judgments about the site. Prior research has shown that subjects will rely on both extrinsic (VAP) and intrinsic (security features) cues when making judgments of learning (Castel 2008). Therefore:

*H3: The interaction of Website VAP cues and Security Feature cues will result in higher consumer CV and PV than Website VAP or Security Features alone, making it the strongest predictor of truthful disclosure of information of the three.*

## **METHOD**

### **Study One**

The first research study will be experimental in nature, taking place in a large, northwestern state university. A 2x2 controlled experiment will be designed to explore the relationship between security features (high-low) and VAP (high-low) on an individual's truthful disclosure of information. The experiment will be conducted using mock-up web interfaces (see Figure 2) that vary the high/low characteristics of security features and VAP. Subjects will be instructed that they are evaluating a website for a local company selling sports memorabilia. They will be exposed to the interfaces and led through a shopping and check-out simulation task. During check-out, various demographic requests will be made. A post-test survey will be

administered to measure how truthful subjects were in their information disclosures and to gauge likelihood of other personal disclosures based on their interaction with the site. Subjects will be debriefed after conclusion of the experiment.

The first independent variable tested will be security features operationalized through security policy statements, check-out security banners, and security verification seals. One website will display verification seals, a clear, thorough security statement, and a graphical banner at check-out that promotes the site’s secure systems. The other site will have no web seals or security banner, and will have a more vague, non-committal security statement. The second independent variable tested will be VAP operationalized through one of two website interfaces. The first will be a high quality website professionally created with graphics, a simple, easily navigated layout, and an official looking check-out page. The second site will contain the same information as the first, but will have very low quality in design and VAP. Control variables for the experiment include Age, Gender, and whether or not demographic information is required to be provided to the site at the checkout page.

Taken together, the interfaces will allow exposure of treatment groups to sites with a mixture of both high/low security and high/low VAP. Random assignment of subjects will limit systematic biases. Subjects will be taken from an undergraduate introductory information systems class from a large university in the United States. Student subjects will participate in the experiment in a controlled laboratory setting and will receive extra credit for their involvement in the study. Research has shown that internet users between the ages of 18 and 32 are among the most active consumer groups of online shoppers, so we believe this is an appropriate sample for the study (Jones and Fox 2009).

**Study Two**

The second study will be identical to the first study, but will take place in a field setting utilizing a snowball sample (Coleman 1958). Students from a distance introductory information systems class will act as seeds for the snowball sample, first being exposed to the shopping simulation task and post-test survey. Upon completion, the student subject will contact three non-students outside of their home to participate in the experiment. Although one limitation of snowball sampling is the lack of completely random samples of subjects, findings can offer more generalizable insights (Salganik and Heckathorn 2004).

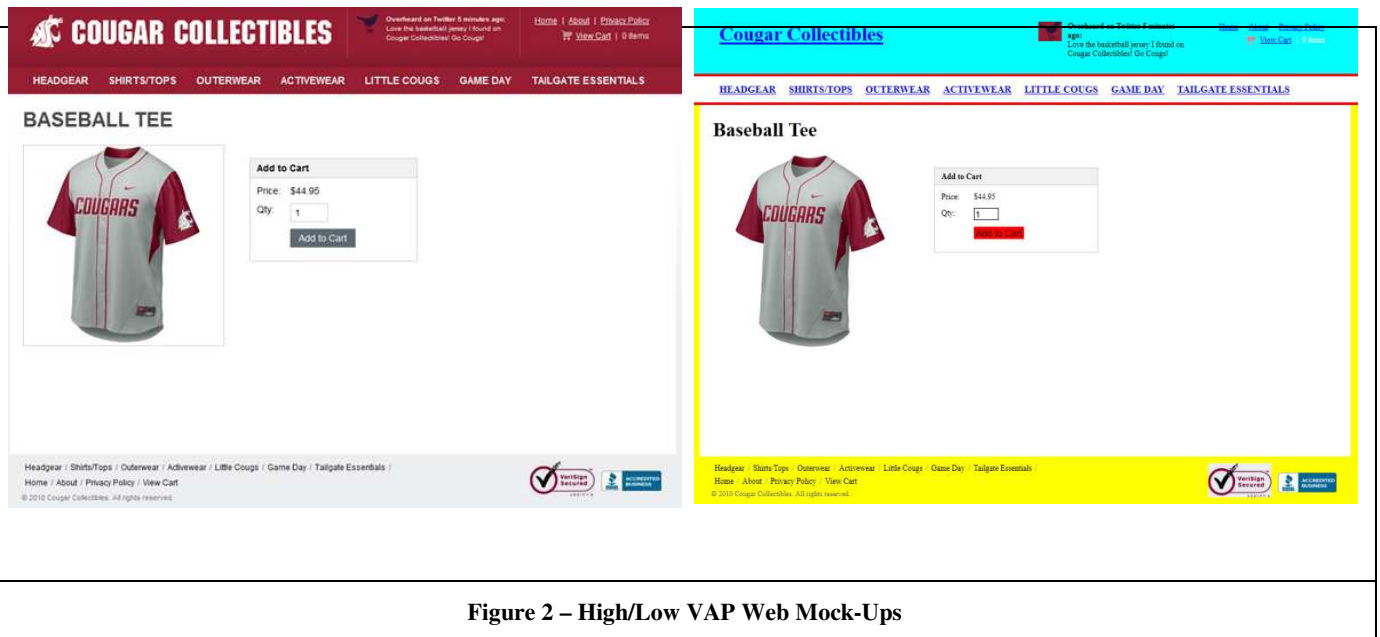


Figure 2 – High/Low VAP Web Mock-Ups

**DISCUSSION**

The proposed research will extend CUT theory. Although there has been much investigation of VAP and security influences on information disclosure, CUT has yet to be applied to this area. From the CUT perspective, we believe that VAP cues will clearly be better predictors of truthful information disclosure than security cues of the site. Finite web design resources may need to be dedicated to VAP over security as VAP is posited to be the more important cue for achieving truthful disclosure. This will be a consideration to website designers as high VAP means higher quality graphics requiring more bandwidth.

There has been no data collection on this experiment. Initial data collection for study one is slated for early Spring 2011. The snowball sample in study two will take place soon after results of study one are collected. We hope to share these results and their contribution to CUT at the conference should this paper be accepted.

## LIMITATIONS AND CONCLUSIONS

Although this study has the potential to offer some interesting theoretical insights into CUT and e-commerce disclosures, it is not without limitations. First, the use of experimental website interfaces will give a certain amount of artificiality to the study. For more validity of the findings, the experiment should be run using actual e-commerce sites in a non-laboratory setting. Second, the use of college students as subjects is often cited as a validity issue (Peterson 2001; Sears 1986). However, as stated earlier, we believe that college students represent an accurate view of the online consumer. Homogeneity of the sample concerns could be addressed in another study using live websites and a snowball sample.

The proposed study provides academics an opportunity to extend the present model by addressing different intrinsic or extrinsic cues to determine their influence on information disclosure. Another interesting avenue for future research would be to bring the variable of *organization quality* into the model and see how website characteristics affect a users' perception of the organization itself.

## REFERENCES

1. Agrawal, R., and Srikant, R. 2000. "Privacy-Preserving Data Mining," SIGMOD Rec. (29:2), 2000, pp 439-450.
2. Altman, I., and Taylor, D.A. 1973. *Social Penetration: The Development of Interpersonal Relationships*. Oxford, England: Holt, Rinehart and Winston New York.
3. Berendt, B., Günther, O., and Spiekermann, S. 2005. "Privacy in E-Commerce: Stated Preferences Vs. Actual Behavior," *Communications of the ACM* (48:4), 2005, p 106.
4. Bucy, E.P., Lang, A., Potter, R.F., and Grabe, M.E. 1999. "Formal Features of Cyberspace: Relationships Between Web Page Complexity and Site Traffic," *Journal of the American Society for Information Science* (50:13), 1999, pp 1246–1256.
5. Castel, A.D. 2008. "Metacognition and Learning About Primacy and Recency Effects in Free Recall: The Utilization of Intrinsic and Extrinsic Cues When Making Judgments of Learning," *Memory & cognition* (36:2), 2008, p 429.
6. Chatterjee, S., Heath, T.B., and Mishra, D.P. 2002. "Communicating Quality Through Signals and Substantive Messages: The Effects of Supporting Information and Need for Cognition.," *Advances in Consumer Research* (29:1), January 2002, pp 228-229.
7. Coleman, J.S. 1958. "Relational Analysis: The Study of Social Organizations with Survey Methods," *Human Organization* (17:4), 1958, pp 28–36.
8. Collins, N.L., and Miller, L.C. 1994. "Self-Disclosure and Liking: A Meta-Analytic Review.," *Psychological Bulletin* (116:3), 1994, pp 457-475.
9. Conti, G., and Sobiesk, E. 2007. "Proceedings of the 3rd Symposium on Usable Privacy and Security," in: *Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, Pennsylvania: ACM, pp. 112-121.
10. Cormier, K.A. 1999. "Developing a Web Site-Med Resorts' Experience," *TMA Journal* (19), 1999, pp 66–68.
11. Cox, D.F. 1967. "Risk Taking and Information Handling in Consumer Behavior," in: *Risk taking and information handling in consumer behavior*. Boston, MA: Division of Research, Graduate School of Business Administration, Harvard University, pp. 641-667.
12. Dawar, N., and Parker, P. 1994. "Marketing Universals: Consumers' Use of Brand Name, Price, Physical Appearance, and Retailer Reputation as Signals of Product Quality," *The Journal of Marketing* (58:2), April 1994, pp 81-95.
13. Goodwin, C. 1991. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing* (10:1), Spring 1991, pp 149-166.
14. Grossman, J. 2008. "Five User-Customizable Web Site Security Features," in: *IEEE Security and Privacy*. pp. 79-81.

15. Hoffman, D.L., Novak, T.P., and Peralta, M. 1999. "Building Consumer Trust Online," *Communications of the ACM* (42:4), 1999, pp 80–85.
16. Hoque, A.Y., and Lohse, G.L. 1999. "An Information Search Cost Perspective for Designing Interfaces for Electronic Commerce," *Journal of Marketing Research* (36:3), August 1999, pp 387-394.
17. Hui, K.L., Teo, H.H., and Lee, S. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), 2007, pp 19–33.
18. Hui, K., Tan, B.C.Y., and Goh, C. 2006. "Online Information Disclosure: Motivators and Measurements," *ACM Trans. Internet Technol.* (6:4), 2006, pp 415-441.
19. Joinson, A.N. 2001. "Self-Disclosure in Computer-Mediated Communication: The Role of Self-Awareness and Visual Anonymity," *European Journal of Social Psychology* (31:2), 2001, pp 177–192.
20. Joinson, A.N., and Paine, C.B. 2007. "Self-Disclosure, Privacy and the Internet," *Oxford handbook of Internet psychology*, 2007, pp 237–52.
21. Jones, S., and Fox, S. 2009. "Generations Online in 2009," Retrieved April 19, 2010 from <http://www.pewinternet.org/Reports/2009/Generations-Online-in-2009.aspx>, Pew Internet & American Life Project.
22. Jourard, S.M. 1964. *The Transparent Self: Self-Disclosure and Well-Being*. Princeton, NJ: Van Nostrand.
23. Jourard, S.M. 1971. *Self-Disclosure: An Experimental Analysis of the Transparent Self*. Oxford, England: Wiley-Interscience New York.
24. Lindgaard, G., Fernandes, G., Dudek, C., and Brown, J. 2006. "Attention Web Designers: You Have 50 Milliseconds to Make a Good First Impression!," *Behaviour & Information Technology* (25:2), 2006, p 115.
25. Liu, C., Marchewka, J.T., Lu, J., and Yu, C. 2005. "Beyond Concern--a Privacy-Trust-Behavioral Intention Model of Electronic Commerce," *Information & Management* (42:2), January 2005, pp 289-304.
26. Longstreet, P. 2010. "2010 43rd Hawaii International Conference on System Sciences," in: *43rd Hawaii International Conference on System Sciences*. Honolulu, Hawaii, USA: pp. 1-7.
27. Lowry, P.B., Vance, A., Moody, G., Beckman, B., and Read, A. 2008. "Explaining and Predicting the Impact of Branding Alliances and Web Site Quality on Initial Consumer Trust of E-Commerce Web Sites," *Journal of Management Information Systems* (24:4), 4, 2008, pp 199-224.
28. McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), September 1, 2002, pp 334-359.
29. Metzger, M.J. 2006. "Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure," *Communication Research* (33:3), June 1, 2006, pp 155-179.
30. Milne, G.R., and Culnan, M.J. 2004. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing* (18:3), 2004, pp 15–29.
31. Milne, G.R., and Gordon, M.E. 1993. "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy & Marketing* (12:2), Fall 1993, pp 206-215.
32. Miyazaki, A., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *Journal of Consumer Affairs* (36:1), 2002, pp 28-49.
33. Miyazaki, A.D., and Fernandez, A. 2000. "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing* (19:1), Spring 2000, pp 54-61.
34. Moon, Y. 2000. "Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers," *Journal of Consumer Research* (26:4), March 1, 2000, pp 323-339.
35. Nielsen, J. 1999. "User Interface Directions for the Web," *Commun. ACM* (42:1), 1999, pp 65-72.
36. Norberg, P.A., Horne, D.R., and Horne, D.A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* (41:1), 2007, p 100.
37. Olson, J.C. 1972. "Cue Utilization in the Quality Perception Process: A Cognitive Model and an Empirical Test," *ETD Collection for Purdue University*, 1972.
38. Olson, J. C., and Jacoby, J. (1972) "Cue Utilization in the Quality Perception Process," in Venhatesan, M. (Ed.) *Proceeding of the Third Annual Conference of the Association For Consumer Research*, Iowa City, Association for Consumer Research, pp. 167-179.



39. Peterson, R.A. 2001. "On the Use of College Students in Social Science Research: Insights from a Second Order Metaanalysis," *Journal of Consumer Research* (28:3), December 1, 2001, pp 450-461.
40. Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), Spring 2000, pp 27-41.
41. Privacy Rights Clearinghouse. 2010. "Chronology of Data Breaches." Retrieved April 17, 2010, from <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
42. Ranganathan, C., and Ganapathy, S. 2002. "Key Dimensions of Business-to-Consumer Web Sites," *Information & Management* (39:6), May 2002, pp 457-465.
43. Richardson, P.S., Dick, A.S., and Jain, A.K. 1994. "Extrinsic and Intrinsic Cue Effects on Perceptions of Store Brand Quality," *The Journal of Marketing* (58:4), October 1994, pp 28-36.
44. Riegelsberger, J., Sasse, M.A., and McCarthy, J.D. 2003. "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems," in: *Proceedings of the SIGCHI conference on Human factors in computing systems*. Ft. Lauderdale, Florida, USA: ACM, pp. 121-128.
45. Salganik, M.J., and Heckathorn, D.D. 2004. "Sampling and Estimation in Hidden Populations Using Respondent-Driven Sampling," *Sociological Methodology* (34:1), 12, 2004, pp 193-240.
46. Sears, D.O. 1986. "College Sophomores in the Laboratory: Influences of a Narrow Data Base on Social Psychology's View of Human Nature.," *Journal of Personality and Social Psychology* (51:3), 1986, pp 515-530.
47. Sheehan, K.B., and Hoy, M.G. 2000. "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing* (19:1), Spring 2000, pp 62-73.
48. Sovern, J. 1999. "Opting in, Opting Out, or No Options at All: The Fight for Control of Personal Information," *Wash. L. Rev.* (74), 1999, p 1033.
49. Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "Proceedings of the 3rd ACM Conference on Electronic Commerce," in: *Proceedings of the 3rd ACM conference on Electronic Commerce*. p. 47.
50. Weisband, S., and Kiesler, S. 1996. "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Common Ground," in: *Proceedings of the SIGCHI conference on Human factors in computing systems: common ground*. Vancouver, British Columbia, Canada: ACM, pp. 3-10.
51. White, T.B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14:1/2), 2004, pp 41-51.
52. Zeithaml, V.A. 1988. "Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence," *The Journal of Marketing* (52:3), July 1988, pp 2-22.