

10-2014

## Effects of perceived privacy protection: does reading privacy notices matter?

Xiaojing Sheng

*University of Texas Rio Grande Valley*, [xiaojing.sheng@utrgv.edu](mailto:xiaojing.sheng@utrgv.edu)

Penny M. Simpson

*The University of Texas Rio Grande Valley*

Follow this and additional works at: [https://scholarworks.utrgv.edu/marketing\\_fac](https://scholarworks.utrgv.edu/marketing_fac)



Part of the [Marketing Commons](#)

---

### Recommended Citation

Sheng, X. and Simpson, P.M., 2014. Effects of perceived privacy protection: does reading privacy notices matter?. *International Journal of Services and Standards*, 9(1), pp.19-36. <https://doi.org/10.1504/IJSS.2014.061059>

This Article is brought to you for free and open access by the Robert C. Vackar College of Business & Entrepreneurship at ScholarWorks @ UTRGV. It has been accepted for inclusion in Marketing Faculty Publications and Presentations by an authorized administrator of ScholarWorks @ UTRGV. For more information, please contact [justin.white@utrgv.edu](mailto:justin.white@utrgv.edu), [william.flores01@utrgv.edu](mailto:william.flores01@utrgv.edu).

**Effects of perceived privacy protection: Does reading privacy notices matter?**

Xiaojing Sheng  
Assistant Professor of Marketing  
College of Business Administration  
The University of Texas-Pan American  
1201 W. University Blvd.  
Edinburg, TX 78539  
Phone: 956.665.3317  
Fax: 956.665.3312  
Email: shengx@utpa.edu

Penny M. Simpson\*  
Professor of Marketing  
College of Business Administration  
The University of Texas-Pan American  
1201 W. University Blvd.  
Edinburg, TX 78539  
Phone: 956.665.2829  
Fax: 956.665.3312  
Email: pmsimpson@utpa.edu

\*Corresponding author

### **Effects of perceived privacy protection: Does reading privacy notices matter?**

Many consumers do not read privacy notices despite the fact that websites post privacy notices to address consumers' long-standing concerns about privacy protection on the Internet. To understand why consumers do not read privacy notices the impact of reading (or not reading) privacy notices on the found effect of privacy notices, data were collected from 137 readers of privacy notices and 97 nonreaders of privacy notices. This research's test of the moderating effects of reading (or not reading) privacy notices found that perceived privacy protection positively affected trust and negatively affected perceived information risk and that the negative effect of perceived privacy protection on perceived information risk became stronger for privacy notice readers. This research also developed a typology of reasons why consumers read and do not read privacy notices.

## **Effects of perceived privacy protection: Does reading privacy notices matter?**

### **Introduction**

Consumers are increasingly turning to the Internet and World Wide Web to purchase goods and services (Punj, 2012) because online shopping empowers them with fun, control, and freedom (Wolfenbarger and Gilly, 2001). Recent statistics show that U.S. retail e-commerce sales for the third quarter of 2013 totaled \$67.0 billion, an increase of 17.3 percent from the same quarter of 2012 (U.S. Census of Bureau News, 2013). Despite the benefits and an upward trend in online shopping, consumers' concerns about the privacy of their personal information (e.g., Becker, 2003), privacy invasion via the Internet (e.g., Choi et al., 2005), and occurrences of Internet fraud (e.g., Koong et al., 2008) remain. In fact, research shows that privacy concerns prevent some consumers from engaging in monetary transactions and disclosing personal information on the Internet (Heirman et al., 2013) and that privacy and security protection is one of the most important attributes influencing consumers' inclination to use Internet banking services (Poon et al., 2009). Studies also find that consumers' perceived risk in online shopping is positively related to their concerns about privacy protection (Miyazaki and Fernandez, 2001) and that privacy concern is a frequently cited reason for not buying online (Forsythe and Shi, 2003). Moreover, privacy concerns cost marketers opportunities to gather consumer information, one of the most important strategic assets of a firm (Xie et al., 2006).

Privacy refers to "the protection of individually identifiable information on the Internet" (Bart et al., 2005). Privacy notices are intended to address consumers' privacy concerns about an organization's data collection and use practices by providing information regarding: (1) what personal information is collected and how the information collected will be used, (2) whether the information collected will be shared with third parties, (3) choices regarding the collection, use,

and distribution of personal information, (4) security of the information being collected, and (5) consumers' access to the information being collected (FTC Report, 1999; 2012). Despite the value of privacy notices to alleviate consumers' privacy concerns and to serve as an organization's accountability function regarding consumers' privacy protection, research shows that many consumers do not read privacy policies. Milne and Culnan (2004) report that about 45% of respondents in their study never or rarely read online privacy notices. More recently, an article in *Consumer Reports* shows that 13 million Facebook users did not know about Facebook's privacy tools that can help them protect and control their privacy (Consumer Reports, 2012). So why do some consumers not read privacy notices while others do, even though they may care deeply about online privacy protection?

Relevant literature on privacy notices was systematically reviewed in terms of the operationalization of privacy notices, outcome variables examined, methodology used, and major research findings. Tables 1 and 2 summarize that literature and reveal three major themes. One research stream focuses on effects of privacy notices on outcome variables such as trust, privacy concerns, personal information provision, probability of making a purchase from a website, and perceived fairness of an organization (see Table 1). Another research stream examines the influence of seals of approval, privacy seals, privacy warnings, and third-party certification on variables such as privacy concerns, personal information provision, and patronage decisions (see also Table 1). The third stream centers on analyzing the content of privacy notices for readability, length and complexity, and whether an organization is compliant with FTC's fair information practices (see Table 2).

[Insert Tables 1 and 2 about here]

These studies have provided many insights into privacy notices and related constructs. However, little effort has been directed towards an understanding of why consumers read or do not read privacy notices. A notable exception is Milne and Culnan's (2004) study in which the authors identified circumstances under which consumers read privacy notices on a website such as first-time users of the website or when asked for personal information. But the reasons for reading privacy notices have not been developed into an instructive classification schema in the literature nor are reasons why consumers do not read the notices explained. As such, an objective of this research is to derive a typology of reasons why consumers read and do not read privacy notices to provide e-tailers guidance in their website privacy notices practices.

Moreover, experiments and surveys are the commonly used methodology in studies examining the effect of privacy notices on trust and other outcome variables (see Table 1). Study participants were either arbitrarily instructed to read privacy notices in an experiment or surveyed about perceptions of privacy notices in a survey-based study with the assumption that the privacy notice was read. As a result, the studies finding effects of privacy notices did not differentiate between consumers who normally read privacy notices when using websites on the Internet and those who do not. The study by Arcand et al. (2007) is a point of departure. The authors compared study participants' perceptions of control over privacy and trust in a web merchant between the group who actually read the privacy notice (i.e., those who clicked on the privacy notice link) and the other group who self-claimed to have read the notice. But the question still remains as to whether privacy notices play an equally important role in influencing trust and other outcome variables for consumers who normally read privacy notices and for those who do not. Therefore, another objective of this research is to address this research deficiency by investigating the moderating effect of reading (or not reading) privacy notices.

## Hypotheses

### *Effects of perceived privacy protection on trust, perceived information risk, and intention*

As summarized in Table 1, research has substantiated the positive effect of privacy notices on consumer trust. Yet evidence also suggests that many consumers either do not read privacy notices (Milne and Culnan, 2004) or they do not fully understand its content (Milne et al., 2006). Given this, consumers' overall perception of the extent to which their privacy is protected at a website becomes an important piece of information in evaluating the website's trustworthiness. In fact, studies have demonstrated that in addition to privacy notices, perceptions of website design investments (Schlosser et al., 2006), brand reputation (Chen et al., 2010), and where privacy information is displayed on a website (Tsai et al., 2011) signal how well privacy is protected, which ultimately determines trust towards the website. Following this logic, consumers should trust a website more when the website is perceived as offering greater privacy protection (referred to as perceived privacy protection throughout). Therefore:

H1. Perceived privacy protection at a website positively affects trust in the website.

Information risk is related to privacy concerns and refers to the uncertainty associated with providing others with personal information which may be exposed on the Internet (Bart et al., 2005). Researchers point out that risk perceptions and trust are closely related (Mayer et al., 1995) and that perceived risk is a necessary antecedent for trust to be operative (Mitchell, 1999). Moreover, research shows that reduced risk perceptions increase trust (Jarvenpaa et al., 1999). Therefore, the positive effect of perceived privacy protection on trust proposed in H1 should also be channeled through perceived information risk such that perceived privacy protection will reduce information risk perceptions and that reduced information risk perceptions will lead to increased consumer trust. Formally stated:

H2. Perceived privacy protection at a website negatively affects perceived information risk at the website.

H3. Perceived information risk at a website negatively affects trust in the website.

Empirical evidence provides extensive support for the positive effect of trust on behavioral intentions such as intention to purchase from an online retailer (Pavlou, 2003), to recommend and register at a website (Bart et al., 2005), and to provide personal information to an e-tailer (Wang et al., 2004). Therefore:

H4. Trust in a website positively affects intention to return to the website.

*Moderating effects of reading (or not reading) privacy notices*

Consumers who read privacy notices show motivation for knowing if and how their information is protected. Consumer research suggests that motivation increases attention to and comprehension of relevant information and produces more stable and enduring attitudes (Celsi and Olson, 1988; Petty et al., 1983). Following this reasoning, consumers who read privacy notices will likely be more attentive than those who do not to information regarding privacy protection at a website. Privacy notice readers will also likely be more active in processing the information regarding the trustworthiness of and potential information risk at the website. This suggests that the hypothesized effects of perceived privacy protection on trust and perceived information risk will become stronger when consumers read privacy notices. Thus:

H5. The positive effect of perceived privacy protection on trust will be stronger for privacy notice readers than for nonreaders.

H6. The negative effect of perceived privacy protection on perceived information risk will be stronger for privacy notice readers than nonreaders.

Hypotheses 1-6 are depicted in Figure 1.



[Insert Figure 1 about here]

## **Method**

### *Data collection and procedure*

Data were collected by an independent research company that specializes in recruiting participants for Internet market research and no known attempt was made to ensure that the study sample was representative of all Internet users. Thus, the study results are considered exploratory only. Participation in the study was voluntary and respondents were paid for their participation in the study.

Participants were prescreened to insure no prior experience with the website shopping.com. Qualified participants were instructed to first read a simulated purchase scenario and were then directed to www.shopping.com and asked to navigate the website for a digital camera priced between \$80 and \$120 that they might consider buying in the near future. Upon completing the search task, participants were then led to an online survey that captured the major constructs of interest for this research. An existing website was used to provide participants with a realistic, online environment in which they could browse and search on the Internet as they would normally.

A total of 234 participants completed the questionnaire. More than half of the respondents were male (55.1%), Caucasian (72.2%), had an income less than \$50,000 (57.9%), and some (38.9%) had a college degree. 20.1% of the respondents were younger than 24 years of age, 63.1% were between 25 and 64, and 16.7% were older than 65 years of age. The participants seem to be Internet savvy, with 89% having more than 5 years of Internet use experiences.

### *Measures*

Measures used in this study were developed based on previously validated scales (Bart et al., 2005; Schlosser et al., 2006; Wang et al., 2004). All items were assessed using 5-point Likert or Likert-type scales (see Table 3). Perceived privacy protection was measured with four items intended to capture perceptions of how well privacy is protected at a website. Trust reflects the overall evaluation of the trustworthiness of a website and was measured with five items. Perceived information risk measures an individual's perception of how risky it would be for the individual to provide personal information on a website and was measured with six items. Intention to return assesses the likelihood of returning and reusing the website and was measured with four items. The survey also asked participants to indicate whether they normally read privacy notices when visiting websites and to provide reasons why they do or do not read privacy notices.

[Insert Table 3 about here]

## **Results**

### *Measurement validity*

Confirmatory factor analysis using AMOS version 21 was conducted to assess measurement validity. The revised measurement model after dropping three items with high modification indices showed good fit to the data:  $\chi^2/df=1.69$ , GFI=0.92, CFI=0.98, RMSEA=0.05. As summarized in Table 3, the results show that convergent and discriminant validity and reliability of the constructs were supported by correct loadings of measurement items onto their intended constructs, substantial factor loadings, Cronbach's  $\alpha$  values above 0.70 (Nunnally, 1978) and composite reliability values greater than 0.70 (Hair et al., 2009). The result that each construct's average variance extracted (AVE) is well above the recommended 0.5 (Bagozzi and Yi, 1988; Fornell and Larcker, 1982) and that the square root of the AVE is greater

than the correlations between the construct and others further supports the constructs' discriminant validity.

### *Hypothesis testing*

Structural equations modeling with AMOS version 21 was used to test hypotheses and results, as summarized in Table 4, show that the structural model fit the data well:  $\chi^2/df=1.68$ , GFI=0.92, CFI=0.98, RMSEA=0.05. Perceived privacy protection positively affected trust ( $\beta=0.54, p<0.001$ ) and negatively affected perceived information risk ( $\beta=-0.13, p=0.04$ ), thus supporting H1 and H2. The results also show that perceived information risk negatively affected trust ( $\beta=-0.11, p=0.02$ ) and that trust positively affected intention to return ( $\beta=0.27, p<0.001$ ), supporting H3 and H4.

Model comparisons between privacy notice readers and nonreaders were conducted to test whether readers differ from nonreaders with regards to the effect of perceived privacy protection on trust and on perceived information risk as predicted in hypotheses 5 and 6. To do so, the sample was first split into two groups: the readers group of 137 participants who responded that they normally read privacy notices and the nonreaders group of 97 participants who do not read privacy notices. To test H5, a model comparison was performed between the structural model with free parameter estimates (unconstrained model) and the model with an equality constraint imposed on the path between perceived privacy protection and trust (constrained model). The results show that the difference between these two models was not significant,  $\Delta\chi^2/\Delta df=0.41, p=0.52$ . Therefore, privacy notice readers did not significantly differ from nonreaders in terms of the magnitude of the positive effect of perceived privacy protection on trust. As such, H5 was not supported.

The same procedure was used in testing H6. Specifically, a model comparison was performed between the structural model with free parameter estimates (unconstrained model) and the model with an equality constraint imposed on the path between perceived privacy protection and perceived information risk (constrained model). The results show that the unconstrained model had a slightly better model fit ( $\chi^2=338.45$ ,  $df=200$ ,  $\chi^2/df=1.69$ , GFI=0.853, CFI=0.962, and RMSEA=0.055) than the constrained model ( $\chi^2=345.99$ ,  $df=201$ ,  $\chi^2/df=1.72$ , GFI=0.850, CFI=0.960, and RMSEA=0.056) and that the difference between these two models is significant,  $\Delta\chi^2/\Delta df=7.54$ ,  $p=0.006$ . This verifies the significant difference between the readers group and the nonreaders group in relation to the negative effect of perceived privacy protection on perceived information risk. The estimated  $\beta$  coefficient is -0.29 ( $p=0.002$ ) for the readers group and -0.06 ( $p=0.51$ ) for the nonreaders group, meaning that perceived privacy protection significantly reduced readers' perceived information risk but this effect did not hold for nonreaders. Therefore, the results provide partial support for H6.

[Insert Table 4 about here]

#### *Additional analysis*

Responses to the open-ended questions that asked participants to explain why they read or do not read privacy notices were analyzed. The analysis produced three broad categories of responses (see Table 5 for categories, subcategories, and exemplars of comments). One category, labeled "individual perspective", included comments reflective of the perspective of the individual who chose to read or not to read privacy notices. Another category, labeled "about the privacy notice", is about the privacy notice itself such as its content and location. The third category, labeled "about the context", deals with the specific context within which an individual will read or not read privacy notices. Within those categories, subcategories of responses

emerged so that all comments could be categorized (inclusiveness) but would fit into only one category (exclusiveness) as recommended by Gorden (1992). Separately, the authors categorized each comment then compared results. Differences were satisfactorily agreed upon for a 100% interrater reliability. Some respondents' comments expressed more than one reason for reading or not reading privacy notices resulting in 97 respondents giving 121 reasons for reading notices and 79 respondents providing 93 reasons for not reading them.

[Insert Table 5 about here]

Why read privacy notices? Within the category of individual perspective, the predominant reason for reading privacy notices was concern about private information being shared or sold (29.8%). Other reasons given include: to be informed (16.5%), concerns for the safety and security of personal information (14.9%), distrust of websites in general (11.6%), and to be in control (9.1%). Reading privacy notices and other matter was a common practice for some respondents (7.4%). Factors related to the privacy notice itself such as content and location was a reason for others to read the notice (7.4%). Finally, 3.3% of the comments were related to prior bad experiences with hacking or identity theft.

Why not read privacy notices? Reasons given for not reading privacy notices under the category of individual perspective include: no time or interest (38.7%), a lack of control (10.8%), using other self-protection strategies (7.5%), and having a trusting nature (2.2%). The privacy notice itself was a reason for some respondents not to read the notice. Some noted the notice's complexity, length, and small print as reasons not to read it (28%) and others said the notice was hard to find (2.2%). Finally, some respondents did not read the notice because they trusted the website (12.9%).

## Discussion

This research makes several contributions. First, the systematic review of relevant research on privacy notices makes an important contribution to the literature by integrating previous studies of privacy notices based on the operationalization of privacy notices, outcome variables examined, methods used, and research findings. Second, this research adds to the extant literature on privacy notices by identifying perceived privacy protection—overall perceptions of how protective a website is regarding information privacy—as a variable that increased trust and reduced information risk perceptions. The finding that reduced information risk perceptions led to greater trust which, in turn, led to greater intention to return to a website is consistent with findings from previous studies that examined the relationship between perceived information risk, trust, and intentions (Bart et al., 2005; Jarvenpaa et al., 1999).

A third contribution is testing the moderating effect of reading (or not reading) privacy notices which has been largely ignored by past research. The result that perceived privacy protection positively affected trust regardless of whether the consumer is a privacy notice reader or nonreader, as indicated by the lack of support for the moderating effect, further speaks to the importance of perceived privacy protection as a mechanism for building consumer trust. The finding that the negative effect of perceived privacy protection on perceived information risk was stronger for readers of privacy notices than for nonreaders confirms earlier research findings that more motivated consumers tend to process relevant information more actively (Celsi and Olson, 1988; Petty et al., 1983). This research also adds to our understanding that the negative impact of perceived privacy protection on perceived information risk can be strengthened when consumers are readers of privacy notice. This finding has practical implications as well. Because perceived privacy protection was less effective in alleviating nonreaders' perceived information risk,

website developers could segment users based on whether they normally read privacy notices and have different website platforms for readers and nonreaders of privacy notices.

Additionally, web developers should encourage the reading of privacy notices by making them easier to see and to read to inspire trust in the website.

A fourth contribution is developing a typology of reasons why consumers read and do not read privacy notices. The typology developed in this research complements Milne and Culnan's (2004) study by including reasons why consumers do not read privacy notices and by identifying categories of reasons based on their commonalities. The typology also offers practical guidance. For example, the complexity of most privacy notices was frequently cited as a reason why respondents did not read the notices in our study. This result lends additional support to the findings from previous research (e.g., Milne et al., 2006; Pan and Zinkhan, 2006; Pollach, 2005) and further illustrates the importance of having clear, simple, and short privacy notices as a focus for website content developers.

Another example is that looking for specific information was reported as a reason for reading privacy notices. This result suggests that website content developers should structure privacy notices to address and highlight privacy issues and prominently place the notices on the website for easy accessibility. Moreover, to meet some consumers' needs, website content developers may want to actively encourage their website visitors to 'be informed' and provide assurances to overcome negative past experiences with information misuse or identity theft.

This research is subject to the usual limitations of online survey research. For example, the sample may not be representative of all Internet users so the results may not be generalizable. Also, this research examined visitors to an existing website. The fact that none of the study participants had used the website before should offset concerns about the influence of past use

experience with the website. Nevertheless, future research could use another existing website or build one to test whether effects found in the current research still hold. Future research could also test whether the reasons provided in the typology indeed predict actual behavior of reading (or not reading) privacy notices as could using different products to examine whether the relationships tested in this research vary by product types (e.g., search vs. experience products).

Author Submission



## References

\*Articles preceded with an asterisk are included in the literature review.

Arcand M., Nantel J., Arles-Dufour M. and Vincent, A. (2007) 'The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust', *Online Information Review*, Vol. 31, No. 5, pp.661-681.

Bagozzi, R.P. and Yi, Y. (1988) 'On the evaluation of structural equation models', *Journal of the Academy of Marketing Science*, Vol. 16, No. 1, pp.74-94.

Bart, Y., Shankar, V., Sultan, F., and Urban, G. L. (2005) 'Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study', *Journal of Marketing*, Vol. 69, No. 4, pp.133-152.

Becker, S.A. (2004) 'A usability study of internet privacy policies for state and commercial websites', *International Journal of Services and Standards*, Vol. 1, No. 1, pp.52-68.

Celsi, R. and Olson, J. (1988) 'The role of involvement in attention and comprehension processes', *Journal of Consumer Research*, Vol. 15, No. 2, pp.210-224.

Chen, Y., Chien, S., Wu, J. and Tsai, P. (2010) 'Impact of signals and experience on trust and trusting behavior', *Cyberpsychology, Behavior, and Social Networking*, Vol. 13, No. 5, pp.539-546.

Choi, Y.B., Hyewon S., and Blackburn, J.M. (2005) 'A quantification model using P3P in privacy control for telecommunications service management', *International Journal of Services and Standards*, Vol. 1, No. 4, pp.426-445.

Consumer Reports (2012) *Facebook & your privacy: who sees the data you share on the biggest social network?* Available online at:

<http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm>;

accessed on October 31<sup>st</sup>, 2013.

- Fornell, C. and Larcker, D.F. (1982) 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, Vol. 18, No. 1, pp.39-50.
- Forsythe, S.M. and Shi, B. (2003) 'Consumer patronage and risk perceptions in Internet shopping', *Journal of Business Research*, Vol. 56, No. 11, pp.867-875.
- FTC Report (1999) *Self-regulation and privacy online: a report to congress*. Available online at: <http://www.ftc.gov/os/1999/07/privacy99.pdf>; accessed on October 31<sup>st</sup>, 2013.
- FTC Report (2012) *Protecting consumer privacy in an era of rapid change*. Available online at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>; accessed on October 31<sup>st</sup>, 2013.
- Gorden, R. (1992) *Basic Interviewing Skills*. Itasca, IL: F. E. Peacock.
- Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2009) *Multivariate data analysis*. 7<sup>th</sup> Ed., Englewood Cliffs, NJ: Prentice-Hall.
- Heirman, W, Walrave, M. and Ponnet, K. (2013) 'Predicting adolescents' disclosure of personal information in exchange for commercial incentives: an application of an extended theory of planned behavior', *Cyberpsychology, Behavior, and Social Networking*, Vol. 16, No. 2, pp.81-87.
- Jarvenpaa, S.L., Tractinsky, N. and Saarinen, L. (1999) 'Consumer trust in an Internet store: a cross-cultural validation', *Journal of Computer Mediated Communication*, Vol. 5, No. 2, pp.1-35.
- Koong, K.S., Liu, L.C., Bai, S., and Wei J. (2008) 'Occurrences of internet fraud in the USA', *International Journal of Services and Standards*, Vol. 4, No. 1, pp.33-53.
- Mayer, R.C., Davis, J.H. and Schoorman, F. (1995) 'An integrative model of organizational trust', *Academy of Management Review*. Vol. 20, No.3, pp.709-734.

- 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*, Vol. 18, No.3, pp.15-29.
- Milne, G.R., Culnan, M.J. and Green, H. (2006) 'A longitudinal assessment of online privacy notice readability', *Journal of Public Policy & Marketing*, Vol. 25, No. 2, pp.238-249.
- Mitchell, V.W. (1999) 'Consumer perceived risk: conceptualisations and models', *European Journal of Marketing*, Vol. 331, No. 1, pp.163-195.
- Miyazaki, A.D. and Fernandez, A. (2001) 'Consumer perceptions of privacy and security risks for online shopping', *Journal of Consumer Affairs*, Vol. 35, No. 1, pp.27-44.
- Nunnally, J.C. (1978) *Psychometric Properties*. 2<sup>nd</sup> Ed., New York, NY: McGraw-Hill.
- Pavlou, P.A. (2003) 'Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model', *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp.101-134.
- Petty, R.E., Cacioppo, J.T. and Schumann, D. (1983) 'Central and peripheral routes to advertising effectiveness: the moderating role of involvement', *Journal of Consumer Research*, Vol. 10, No. 2, pp.135-146.
- Poon, W.-C., Yong, G.-F.D., and Lam, W.-H.P. (2009) 'An insight into the attributes influencing the acceptance of internet banking: the consumers' perspective', *International Journal of Services and Standards*, Vol. 5, No. 1, pp.81-94.
- Schlosser, A. E., White, T. and Lloyd, S.M. (2006) 'Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions', *Journal of Marketing*, Vol. 70, No. 2, pp.133-148.

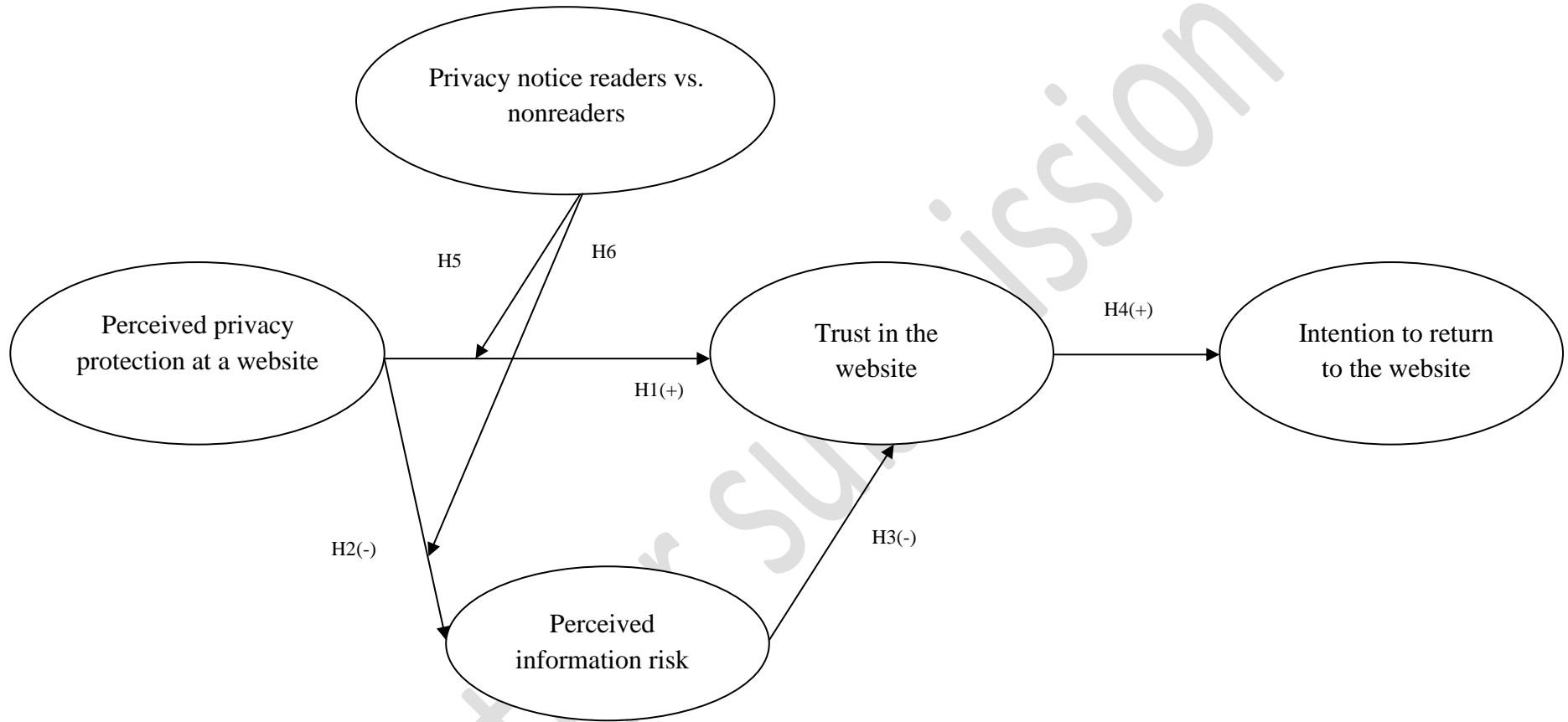
- Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2011) 'The effect of online privacy information on purchasing behavior: an experimental study', *Information Systems Research*, Vol. 22, No. 2, pp.254-268.
- U.S. Census of Bureau News (2013) [online]  
[http://www.census.gov/retail/mrts/www/data/pdf/ec\\_current.pdf](http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf) (Accessed 10 March 2014).
- Wang, S., Beatty, S.E. and Foxx, W. (2004) 'Signaling the trustworthiness of small online retailers', *Journal of Interactive Marketing*, Vol. 18, No. 1, pp.53-69.
- Wolfenbarger, M. and Gilly, M.C. (2001) 'Shopping online for freedom, control, and fun', *California Management Review*, Vol. 43, No. 2, pp. 34-55.
- Xie, E, Teo, H and Wan, W. (2006) 'Volunteering personal information on the Internet: effects of reputation, privacy notices, and rewards on online consumer behavior', *Marketing Letters*, Vol. 17, No. 1, pp.61-74.
- \*Andrade, E.B., Kaltcheva, V. and Weitz, B. (2002) 'Self-disclosure on the web: the impact of privacy policy, reward, and company reputation', *Advances in Consumer Research*, Vol. 29, No. 1, pp.350-353.
- \*Bernard, E. and Makienko, I. (2011) 'The effects of information privacy and online shopping experience in e-commerce', *Academy of Marketing Studies Journal*, Vol. 15 (Supplement), No. 1, pp.97-112.
- \*Culnan, M.J. (2000) 'Protecting privacy online: is self-regulation working?', *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp.20-26.
- \*Hoy, M.G. and Phelps, J. (2003) 'Consumer privacy and security protection on church web sites: reasons for concern', *Journal of Public Policy & Marketing*, Vol. 22, No. 1, pp.58-70.

- \*Larose, R. and Rifon, N.J. (2007) 'Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior', *Journal of Consumer Affairs*, Vol. 41, No. 1, pp.127-149.
- \*Lauer, T. and Deng, X. (2007) 'Building online trust through privacy practices', *International Journal of Information Security*, Vol. 6, No. 5, pp.323-331.
- \*Lee, B.C., Ang, L. and Dubelaar, C. (2005) 'Lemons on the web: A signaling approach to the problem of trust in Internet commerce', *Journal of Economic Psychology*, Vol. 26, No. 5, pp.607-623.
- \*Liu, C., Marchewka, J.T., Lu, J. and Yu, C.S. (2005) 'Beyond concern-a privacy-trust-behavioral intention model of electronic commerce', *Information & Management*, Vol. 42, No. 2, pp.289-304.
- \*Liu, C. and Arnett, K.P. (2002) 'An examination of privacy policies in Fortune 500 web sites', *Mid-America Journal of Business*, Vol. 17, No. 1, pp.13-21.
- \*Meinert, D.B., Peterson, D.K., Criswell, J.R. and Crossland, M.D. (2006) 'Would regulation of web site privacy policy statements increase consumer trust?', *Informing Science Journal*, Vol. 9, pp.123-142.
- \* Meinert, D.B., Peterson, D.K., Criswell, J.R. and Crossland, M.D. (2006) 'Privacy policy statements and consumer willingness to provide personal information', *Journal of Electronic Commerce in Organizations*, Vol. 4, No. 1, pp.1-17.
- \*Milne, G.R. and Culnan, M.J. (2002) 'Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998-2001 U.S. web surveys', *Information Society*, Vol. 18, No. 5, pp.345-359.

- \*Miyazaki, A.D. and Krishnamurthy, S. (2002) 'Internet seals of approval: Effects on online privacy policies and consumer perceptions', *Journal of Consumer Affairs*, Vol. 36, No. 1, pp.28-49.
- \*Mollick, J. S. and Mykytyn, P. P. (2009) 'An empirical investigation on the effects of privacy policies on perceived fairness of online vendors', *Journal of Internet Commerce*, Vol. 8, No. 1/2, pp.88-112.
- \*Nam, C., Song, C., Lee, E. and Park, C. I. (2006) 'Consumers' privacy concerns and willingness to provide marketing-related personal information online', *Advances in Consumer Research*, Vol. 33, pp.212-217.
- \*O'Connor, P. (2007) 'Online consumer privacy: an analysis of hotel company behavior', *Cornell Hotel and Restaurant Administration Quarterly*, Vol. 48, No. 2, pp.183-200.
- \*Pan, Y. and Zinkhan, G.M. (2006) 'Exploring the impact of online privacy disclosures on consumer trust', *Journal of Retailing*, Vol. 82, No. 4, pp.331-338.
- \*Papacharissi, Z. and Fernback, J. (2005) 'Online privacy and consumer protection: an analysis of portal privacy statements', *Journal of Broadcasting & Electronic Media*, Vol. 49, No. 3, pp.259-281.
- \*Pollach, I. (2005) 'A typology of communicative strategies in online privacy policies: ethics, power and informed consent', *Journal of Business Ethics*, Vol. 62, No. 3, pp.221-235.
- \*Pollach, I. (2006) 'Privacy statements as a means of uncertainty reduction in www interactions', *Journal of Organizational & End User Computing*, Vol. 18, No. 1, pp.23-49.
- \*Pollach, I. (2007) 'What's wrong with online privacy policies?', *Communications of the ACM*, Vol. 50, No. 9, pp.103-108.

- \*Sheehan, K.B. (2005) 'In poor health: an assessment of privacy policies at direct-to-consumer web sites', *Journal of Public Policy & Marketing*, Vol. 24, No. 2, pp.273-283.
- \*Vail, M.W., Earp, J.B. and Anton, A.I. (2008) 'An empirical study of consumer perceptions and comprehension of web site privacy policies', *IEEE Transactions on Engineering Management*, Vol. 55, No. 3, pp.442-454.
- \*Wirtz, J., Lwin, M.O. and Williams, J.D. (2007) 'Causes and consequences of consumer online privacy concern', *International Journal of Service Industry Management*, Vol. 18, No. 4, pp.326-348.
- \*Wu, K., Huang, S., Yen, D.C. and Popova, I. (2012) 'The effect of online privacy policy on consumer privacy concern and trust', *Computers in Human Behavior*, Vol. 28, No. 3, pp.889-897.

**Figure 1. Conceptual model**





**Table 1. Summary of literature on the effects of privacy notices, seals, warnings, and third-party certificates**

<b>Literature</b>	<b>Operationalization of privacy notice</b>	<b>Outcome variables</b>	<b>Method</b>	<b>Major findings</b>
Andrade, Kaltcheva, and Weitz (2002)	Privacy policy (completeness of a privacy policy: extensive vs. brief)	Concerns about disclosing personal information	Experiment	A more complete privacy policy reduced self-disclosure concerns.
Bart, Shankar, Sultan, and Urban (2005)	Privacy (perceptions of privacy policies)	Trust	Survey	Privacy positively affected trust in websites where information risk is high.
Bernard and Makienko (2011)	Privacy policy (perceptions of a privacy policy: availability, clarity, credibility, and understandability)	Perceived trustworthiness of an e-tailer; privacy concerns	Survey	Privacy policy positively affected perceived trustworthiness and negatively affected privacy concerns.
Chen, Chien, Wu, and Tsai (2010)	Privacy policy (perceptions of security, information disclosing, and data protection mechanisms)	Trusting beliefs	Survey	Perceptions of privacy policies positively affected all trusting beliefs.
Larose and Rifon (2007)	Privacy warnings Privacy seals	Information disclosure	Experiment	Privacy warnings decreased and seals increased information disclosure intentions; both a warning and a seal had an interaction effect on expected negative consequences.
Lauer and Deng (2007)	Privacy policy (one policy complied with FTC guidelines and the other did no.)	Perceived trustworthiness toward a company	Survey	Stronger policies led to higher trustworthiness (integrity, benevolence, and ability)
Lee, Ang, and Dubelaar (2005)	Privacy policy (presence of a privacy policy vs. absence)	Probability of a purchase	Experiment	A privacy policy increased the probability of a purchase.
Liu, Marchewka, Lu, and Yu (2005)	Privacy policy (measured as perceptions of the four dimensions of a privacy policy)	Trust	Experiment	The privacy policy with all four dimensions led to greater trust.
Meinert, Peterson, Criswell, and Crossland (2006a)	Varied privacy policy notices: the legally mandated policy and voluntary policies with strong, moderate, and weak statements or no policy.	Willingness to provide information	Survey	Strong and legally mandated privacy policies affected willingness to provide information; type of policy most affected willingness to provide financial data.

<b>Literature</b>	<b>Operationalization of privacy notice</b>	<b>Outcome variables</b>	<b>Method</b>	<b>Major findings</b>
Meinert, Peterson, Criswell, and Crossland (2006b)	Three privacy policy statements (strong, moderate, and weak) and no privacy policy.	Willingness to provide information	Survey	A strong privacy policy led to greater willingness to provide information; and familiarity interacted with privacy policy to affect willingness to provide information.
Miyazaki and Krishnamurthy (2002)	Seals of approval	Privacy practices; Information disclosure; Patronage decision	Experiment	A seal positively affected perceived privacy practices; the seal positively affected information disclosure and patronage decisions when shopping risk was high.
Mollick and Mykytyn (2009)	Privacy policy (informed consent, data sharing, and secondary use of data)	Perceived fairness of an organization	Experiment	All three dimensions of the privacy policy positively affected perceived fairness of an organization.
Nam, Song, Lee, and Park (2006)	3 <sup>rd</sup> party certificates	Privacy concerns	Survey	3 <sup>rd</sup> party certificates negatively affected privacy concerns.
Pan and Zinkhan (2006)	Privacy disclosures (presence vs. absence; absence vs. long vs. short privacy notices)	Trust	Experiment	Greater trust in websites when privacy risk was high, with privacy notices being present.
Schlosser, White, and Lloyd (2006)	Privacy statement (strong vs. weak vs. no privacy statement)	Trust	Experiment	Stronger privacy statement led to greater beliefs in benevolence and integrity.
Vail, Earp, and Anton (2008)	Privacy policy (typical privacy policy in paragraph format vs. atypical privacy policy with different presentation formats)	Comprehension; Sharing personal information; Protection	Experiment	Typical privacy policies are more thorough, more difficult to understand but evoked more felt security
Wirtz, Lwin, and Williams (2007)	Privacy policy (misusing personal information, information sharing, and protection of information against unauthorized access)	Privacy concerns	Email-based survey	A privacy policy negatively affected privacy concerns; privacy concerns fully mediated negative effects of the policy on giving false information, using protection technology, and not purchasing from a website.
Wu, Huang, Yen, and Popova (2012)	Privacy policy (perceptions of notice, choice, access, security, and enforcement)	Privacy concerns; Trust	Survey	Access, security, and enforcement negatively impacted privacy concerns; notice, access, and security positively impacted trust.
Xie, Teo, and Wan (2006)	Privacy notices (a secure connection, a privacy policy, and TRUSTe certification)	Provision of personal information	Experiment	Presence of privacy notices positively affected willingness to provide personally information.

**Table 2. Summary of reviewed literature on content analysis of privacy notices**

<b>Literature</b>	<b>Method</b>	<b>Major findings</b>
Culnan (2000)	Evaluated websites regarding personal information collection, frequency of privacy disclosures, and nature of disclosures at the site.	67% of 361 websites posted privacy disclosures with 14% of fair information compliant; nearly one-third did not post any privacy disclosures.
Hoy and Phelps (2003)	Content analysis of 102 randomly selected websites representing Christian churches from all 50 states	99% of the websites collected personal information, but less than 3% posted a privacy policy and 85.6% posted personal information.
Liu and Arnett (2002)	Content analysis of privacy policies posted on Fortune 500 companies' public websites	Of the 497 websites examined, slightly more than 50% have privacy policies and that most privacy policies address information use, collection, and disclosure.
Milne and Culnan (2002)	Content analysis of privacy disclosures from a comparable individual-level-website data from the 1998, 1999, 2000, 2001 web surveys	Websites posting privacy disclosures increased in number; websites posting information practice statements declined in number in 2001; more of the most popular websites voluntarily post privacy disclosures than the general population of websites.
Milne, Culnan, and Greene (2006)	Content analysis of readability of privacy notices on 483 websites in 2001 then 2003	From 2001 to 2003, readability of the examined privacy notices declined while length of the notices increased; privacy notices with privacy seals are more readable.
O'Connor (2007)	Content analysis was conducted on the privacy policies from 97 hotels' websites.	All but one website had a privacy policy; no websites fully complied with the FTC's fair information practices (FIP); the policies were compliant with notice only.
Papacharissi and Fernback (2005)	Content analysis of 97 randomly selected Internet portals' privacy statements	Perceived credibility of privacy statements was positively related to clarity of legal and computer terms, and overall impression of privacy protection; and was negatively related to extensive use of computer terms.
Pollach (2005)	Content analysis of privacy statements from 28 websites using critical linguistic analysis	Four communicative strategies were identified: mitigation and enhancement, obfuscation of reality, relationship building, and persuasive appeals.
Pollach (2006)	Content analysis of 50 privacy policies regarding companies' data handling practices.	66% of privacy policies addressed data collection and sharing and spam policies.
Pollach (2007)	Content analysis of 50 websites' privacy policies about data collection, storage and sharing and marketing communication.	Companies obscure privacy infringements by downplaying the frequency, mitigating questionable practices, and omitting references to themselves when talking about unethical data handling practices.
Sheehan (2005)	Content analysis of the privacy policies on 94 direct-to-consumer branded-drug websites.	93.7% of the websites had a privacy notice; most were compliant with the FTC's FIP about notice but poor with choice, access, and security.

**Table 3. Construct attributes**

Construct and Items	Factor Loadings	Composite Reliability	Cronbach's Alpha	1	2	3	4
<b>1. Perceived privacy protection</b>		.95	.96	.91 <sup>a</sup>			
This website seems to have the technology to protect my privacy.	.91						
This website seems very capable of protecting my privacy.	.97						
It seems that this website invested a great deal of money in privacy protection.	.85						
I believe my privacy is protected at this site.	.91						
<b>2. Perceived information risk</b>		.90	.90	-.14*	.83		
I would feel very safe giving my personal information on this website. †	--						
I would feel very comfortable sharing my personal information on this website. †	--						
I feel uncertain about sharing my personal information on this website.	.78						
It would be very risky for me to share any information on this website.	.89						
My personal information might be misused if I share it on this website.	.86						
This website might sell my personal information to other companies.	.79						
<b>3. Trust</b>		.94	.94	.65**	-.22*	.90	
This website appears to be very trustworthy.	.86						
This website can be relied upon.	.86						
I do not believe the information on this website is correct. †	--						
I am confident that this website can be trusted.	.95						
My overall faith in this website is high.	.92						
<b>4. Intention to return</b>		.95	.95	.17*	-.03	.30**	.91
I would come back to this website again.	.89						
I would never use this website in the future.	.93						
I would recommend this website to my friends.	.91						
I would bookmark this website.	.92						

a: Diagonal elements are square roots of the average variance extracted (AVE), and off-diagonal elements are inter-construct correlations.

\*\* indicate that the correlation is significant at  $p < 0.001$ .

\* indicate that the correlation is significant at  $p < 0.05$ .

† indicate that the items are dropped due to high modification indices.

**Table 4. Summary of hypothesis testing results**

Hypothesis	Results	Supported or not supported
<b>H1:</b> Perceived privacy protection → (+) Trust	$\beta=0.54, p<0.001$	Supported
<b>H2:</b> Perceived privacy protection → (-) Perceived information risk	$\beta=-0.13, p=0.04$	Supported
<b>H3:</b> Perceived information risk → (-) Trust	$\beta=-0.11, p=0.02$	Supported
<b>H4:</b> Trust → (+) Intention to return	$\beta=0.27, p<0.001$	Supported
<b>H5:</b> The positive effect of perceived privacy protection on trust will be stronger for privacy notice readers than nonreaders.	The difference between the constrained and unconstrained model was not significant, $\Delta\chi^2/\Delta df=0.41, p=0.52$ .	Not supported
<b>H6:</b> The negative effect of perceived privacy protection on perceived information risk will be stronger for privacy notice readers than nonreaders.	The difference between the constrained and unconstrained model was significant, $\Delta\chi^2/\Delta df=7.54, p=0.006$ . The negative effect of perceived privacy protection on perceived information risk was significant for privacy notice readers ( $\beta=-0.29, p=0.002$ ) but not significant for nonreaders ( $\beta=-0.06, p=0.51$ ).	Partially supported

**Table 5. Why respondents do or do not read privacy notices**

Category	% Responses	Examples of comments
<b>Why respondents DO read privacy notices</b>		
<i>Individual perspective</i>		
Information concerns	29.8%	I am concerned that companies sell our information.
To be informed	16.5%	To get informed. To know my rights.
Safety concerns	14.9%	I want to be sure that my personal info is safe.
Distrust	11.6%	I don't trust anyone who has access to my personal data, especially when it concerns credit cards & privacy.
To be in control	9.1%	Always know what you are getting yourself into
Always read	7.4%	I was taught to read everything before making purchase or putting any info out on the internet, no matter how secure
<i>About the privacy notice</i>		
Look for specific information	7.4%	I am interested in seeing what the company says about their privacy policies. I am interested in how they share their information with other companies.
<i>About the context</i>		
Bad past experience	3.3%	I want to feel comfortable and trust that my information will be safe, due to the fact I have been hacked twice, when giving my personal info out!!
<b>Why respondents DO NOT read privacy notices</b>		
<i>Individual perspective</i>		
No time/interest	38.7%	Don't have time. No interest. Don't think about it.
Lack of control	10.8%	No server is hack-proof and putting information out on the web is a chance you take.
Other self-protection strategies	7.5%	My computer alerts me to unsafe web sites. I refuse to give out personal info.
Trusting nature	2.2%	It is in my nature to trust people.
<i>About the privacy notice</i>		
Complex statement	25.8%	Privacy policies are long and take too much time to read.
Hard to find	2.2%	On occasion I do read privacy policies, however most times they are not prominent and I do not remember to search for it.
<i>About the context</i>		
Trusted website	12.9%	Trust in the website. No need unless I'm giving out information.