

The Relationship between Privacy Notice Formats and Consumer Disclosure Decisions: A Quantitative Study

Alexys Mercedes Carlton, David Cross

ABSTRACT: *In the Data Era, the future success of many businesses will heavily depend on the business' ability to collect and process consumer personal information. Business leaders must understand and implement practices that increase consumer trust to influence their willingness to disclose their information. The problem addressed by this study is many consumers do not trust online service providers with their personal information, and as a result, have refrained from engaging in online activities. The purpose of this quantitative correlational study was to understand how consumers use privacy notices when deciding to share their personal information with online businesses. A sample of 288 adult privacy pragmatists were randomly assigned to read one of three privacy notice formats, a full-text format, a layered text format, or a standardized table format, and asked to answer a survey. A one-way analysis of variance was used to test the hypotheses. This study $F(8, 55) = 2.08, p = .04$ found a relationship between privacy notice type and consumer trust ($\eta = .22, p = .001$). No relationship was found between privacy notice type and a consumer's perceived protection belief ($\eta = .14, p = .07$), perceived risk belief ($\eta = .05, p = .70$), or likeliness to disclose ($\eta = .11, p = .20$). Practitioners should focus factors that will encourage disclosure collect consumer personal information other than website privacy notice format. Further research is needed to study these relationships in different online contexts and with different populations.*

KEY WORD: *Consumer Personal Information, Online selling, Privacy*

Date of Submission: 25-02-2020

Date of Acceptance: 11-03-2020

I. INTRODUCTION

Most businesses' future success depends on the collection and access to personal data, and this dependency continues to increase (Norman, Pepall, Richards, & Tan, 2016). Big Data is not new; however, it has been fueled recently by advances in and the adoption of cloud-based technologies and Internet of Things. By 2020, it is estimated that there will be over 50 billion connected devices as Internet of Things devices become more prominent (Federal Trade Commission, 2015). A new revolution is occurring in business as industries transition to the Data Era, an era when consumer information becomes a critical business asset and an economic currency. Industries are entering the Data Era at a time when individuals are more concerned about their data privacy. Therefore, it is imperative that businesses understand and implement practices that increase consumer trust to influence their willingness to disclose information.

Statement of the Problem

The problem is that many consumers do not trust online service providers with their personal information. Privacy and security concerns have prevented 45% of American households from completing online activities such as purchasing products and services or using social media (Goldberg, 2016). The continued success of e-commerce requires consumers' willingness to share their personal information. A transparent and readable privacy notice is a factor that influences consumer trust and willingness to disclose personal information. Failure to understand how characteristics of the privacy notice impact a consumer's willingness to disclose personal information online may lead to a continued loss of business opportunity. When consumers do not trust sharing their information online, they are less likely to provide the personal information necessary for the success of online service providers.

Purpose of the Study

The purpose of this quantitative correlational study was to understand how consumers use privacy notices in their decisions whether to share their personal information with online businesses, and ultimately, complete the business transaction. Businesses may experience increased or continued online success by adopting a privacy notice designed to encourage consumers to share personal information.

Research Questions

Previous research found that a readable format can increase a consumer's trust and willingness to disclose information (Ermakova et al., 2014). The length, specificity, and visibility of a privacy notice play a significant role in consumers' perception of the notice's importance and relevance (Capistrano & Chen, 2015):

RQ1. How do consumers view the relationship between privacy notice type and trust?

RQ2. How do consumers view relationship between privacy notice type and their likeliness to disclose personal information?

Hypotheses

H1₀: There is no relationship between privacy notice type and trust.

H1_a: There is a relationship between privacy notice type and trust.

H2₀: There is no relationship between privacy notice type and likeliness to disclose personal information.

H2_a: There is a relationship between privacy notice type and likeliness to disclose personal information.

Research Method

A quantitative, quasi-experimental correlational study was used to examine the possible relationship between a privacy notice format and trust and likeliness to disclose personal information in an eCommerce context.

Population and Sample

The population of this quantitative correlational study were United States adult privacy pragmatists. A power analysis was conducted to determine the minimum sample size of 111 (Faul, Erdfelder, Lang, & Buchner, 2009). Purposeful sampling was used to recruit a total of 288 participants for this study. Participants were recruited using Amazon Mechanical Turk, which is a marketplace where workers are paid for Human Intelligence Tasks (Amazon Web Services, Inc., 2018).

Materials/Instrumentation

The participants were presented with an online shopping scenario in which they would be required to share their contact and credit card information to complete a purchase. Then, participants were instructed to read the privacy notice and answer the survey questions designed to measure how consumers viewed the relationship between privacy notice type and trust, and their likeliness to disclose personal information. The privacy notice format was manipulated at three levels: full-text, layered-text, and standardized table. The participants were randomly assigned to one of the three privacy notice formats.

Data was collected using existing published scales. The general privacy concern scale developed by Motiwalla, Li, and Liu (2014) was used to measure privacy concern. Trust was measured using items adapted from Pan and Zinkhan (2006), who created this scale to understand how online privacy disclosure impact consumer trust. Likeliness to disclose was measured using items adapted from Li et al. (2010).

Operational Definitions of Variables

Likeliness to disclose. The ordinal, dependent variable is defined as the consumer's likeliness to disclose personal information to the company (Li et al., 2010).

Perceived privacy risk. The ordinal, dependent variable is defined "as the degree to which an individual believes that a high potential for loss and/or profit is associated with the release of personal information to a company" (Zhu et al., 2017, p. 428).

Privacy notice format. The nominal, independent variable is defined by the structure or format of the website privacy notice provided to the consumers. There were three privacy notice formats in this study: full-text, layered-text, and standardized table. A full-text notice is a notice that uses natural-language and is full length. A layered-text notice is "a summarized, one-screen privacy policy in a tabular format that links to the full natural-language policy" (Kelley et al., 2010, p. 2). A standardize table notice is "a tabular privacy format designed to enhance user understanding of privacy practices, increase the speed of information finding, and facilitate policy comparisons" (p. 2).

Trust. The ordinal, dependent variable is defined as "the buyer's willingness to be vulnerable to the online marketplace" (Kim & Koo, 2016, p. 1022). Trust was measured to examine whether there is a statistically significant relationship between privacy notice format and trust.

Data Collection and Analysis

All data was collected using an online survey. After data collection was complete, the data was securely imported into Statistical Package for the Social Sciences (SPSS) on secure computer. A one-way analysis of variance (ANOVA) was used to assess the hypotheses and test whether there were statistically significant relationships between the independent variable and dependent variables.

II. RESULTS

The participants were presented with an online shopping scenario in which they would be required to share their contact and credit card information to complete a purchase. The privacy notice format was manipulated at three levels: full-text, layered-text, and standardized. A one-way analysis of variance (ANOVA) was used to test the hypotheses.

Table 1 MANOVA and ANOVA Tests for Scale Scores Based on Privacy Notice Type

Scale	Privacy Notice Type	n	M	SD	η	F	p
Trust Scale ^a					.22	6.75	.001
	1. Full-Text	87	5.38	1.21			
	2. Layered	89	5.38	1.21			
	3. Standardized	105	4.83	1.19			
Likelihood to Disclose Item					.11	1.61	.20
	1. Full-Text	87	5.05	1.49			
	2. Layered	89	5.18	1.34			
	3. Standardized	105	4.83	1.33			

Note. MANOVA Model. Wilks' Lambda: $F(8, 55) = 2.08, p = .04$.

^a Bonferroni post hoc test: $3 < 1, 2 (p = .006)$.

Research question one. Research question one examined if there was a statistically significant relationship between a privacy notice format and a consumer's trust.

Table 1 displays the one-way ANOVA test comparing the three privacy notice groups based on the trust scale. An eta coefficient was included (η , Pearson correlation between a categorical/nominal variable and a continuous variable) to assess the strength of the relationship. Inspection of the table found a significant relationship between privacy notice type and the trust scale ($\eta = .22, p = .001$). The Bonferroni post hoc test found participants in the standardized privacy notice group ($M = 4.83$) to have significantly lower trust scores ($p = .006$) than either the participants in the layered notice group ($M = 5.38$) or the full text notice group ($M = 5.38$). This combination of findings provided support to reject the null hypothesis ($H1_0$) and to accept the alternative hypothesis ($H1_a$).

Research question two. Research question two examined if there was a statistically significant relationship between a privacy notice format and a consumer's likelihood to disclose personal information. Table 1 displays the one-way ANOVA test with the eta coefficient comparing the three privacy notice groups based on the item measuring the likelihood to disclose personal information. Inspection of the table found a nonsignificant relationship between privacy notice type and item measuring the likelihood to disclose personal information ($\eta = .11, p = .20$). This combination of findings provided support to retain the null hypothesis ($H2_0$) and reject the alternative hypothesis ($H4_a$).

Evaluation of the Findings

The results of this study found a statistically significant relationship between privacy notice type and consumer trust. The participants assigned to the standardized privacy notice group were found to have significantly lower trust scores than either the participants in the layered-text notice group or the full-text notice group. There was no significant difference in trust found between the full-text notice group and the layered-text notice group.

The results of this study did not find a relationship between privacy notice type and the participant's likelihood to disclose their personal information. There was no significant difference found in the participant's privacy related costs or their likelihood to disclose across the privacy notice groups.

III. DISCUSSION

Implications

Hypothesis 1. The findings of Hypothesis 1 supported the alternative hypothesis that there is a relationship between privacy notice type and trust ($\eta = .22, p = .001$). The first implication of this finding was the privacy notice format may impact a privacy pragmatic's trust in an e-commerce company. This finding suggested that

certain notice types may increase or decrease trust. Previous research has suggested that the mere presence of a privacy notice and readable or comprehensible notices can increase consumer trust (Erkmakova et al., 2014; Pan & Zinkhan, 2006). The results of Hypothesis 1 further supported the relationship between website privacy notices, including notice type, and consumer trust.

The participants assigned to the standardized table notice group had significantly lower trust scores ($p = .006, p < .05$) than the participants in either the layered-text notice or the full-text notice groups. There was no significant difference in the participants' trust score for the layered-text notice and the full-text notice groups. The second implication of this finding was the privacy pragmatics trusted the e-commerce company that used the standardized table notice less than the other privacy notice types.

Hypothesis 2. The findings of Hypothesis 2 supported the null hypothesis that there is no relationship between privacy notice type and likeliness to disclose personal information. The implication of this finding was a privacy notice type does not impact a privacy pragmatic's likeliness to disclose personal information.

Recommendations for Practice

The results of this study highlight several practical implications. For practitioners, it is important to consider the privacy notice type if the company is focused on increasing consumer trust. A visible privacy notice and the use of either a full-text or layered-text notice may increase consumer trust more than the use of a standardized table format. The results also indicated that these three privacy notice types did not impact the consumer's likeliness to disclose personal information. While the consumers did not trust the company that use the standardized table format as much as the other two formats, these consumers had the same likelihood to disclose personal information. For policymakers, it is important for the Federal Trade Commission and other regulatory bodies to consider how privacy policy format guidance may impact consumer trust.

Recommendations for Future Research

There are several opportunities to extend this research. Researchers could study relationship between the privacy notice format and a consumer's trust in different contexts. Future studies could examine these relationships in other online contexts, such as social media or online dating when they would need to share more intimate information about themselves, such as their pictures or private communications.

Researchers could repeat this study with participants from other countries or cultures. Privacy may be different across cultures. It will be interesting to examine the relationship between privacy notice format and a consumer's trust and privacy calculus in the European Union following the enactment of the GDPR. This study focused on three policy formats. Researchers could repeat this study using additional policy types, such as video formats.

IV. CONCLUSIONS

Consumer information is becoming a critical business asset and an economic currency at a time when individuals are more concerned about their data privacy. Trust has a direct relationship to and may predict intention to disclose personal information. This study highlighted the importance for business to adopt multiple practices that will encourage consumers to disclose personal information. Improvements to the privacy notice, including format, aid in such encouragement, but will not solve the problem online business are facing today. Consumers perform a cost-benefit analysis, to decide whether to share their personal information. The findings of this study increase our understanding of consumer trust and disclosure decisions and add to the body of knowledge by studying how privacy notice types are related to an individual's privacy calculus.

REFERENCES

- [1]. Amazon Web Services, Inc. (2018). Creating a hit. Retrieved from [https:// docs.aws.amazon.com/AWSMechTurk/latest/AWSMechanicalTurkGettingStartedGuide/CreatingAHIT.html](https://docs.aws.amazon.com/AWSMechTurk/latest/AWSMechanicalTurkGettingStartedGuide/CreatingAHIT.html)
- [2]. Capistrano, E. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, 42, 24-31. doi:10.1016/j.csi.2015.04.001
- [3]. Ermakova, T., Baumann, A., Fabian, B., & Krasnova, H. (2014). Privacy policies and users' trust: Does readability matter? Retrieved from <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1141&context=amcis2014>
- [4]. Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39, 175-191.
- [5]. Federal Trade Commission. (2015). Internet of things: Privacy & security in a connected world. Retrieved from <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>
- [6]. Goldberg, R. (2016). Lack of trust in Internet privacy and security may deter economic and other online activities. National Telecommunications and Information Administration. United States Department of Commerce. Retrieved from <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>
- [7]. Kelley, P., Cesca, L., Bresee, J., & Cranor, L. (2010). Standardizing privacy notices: An online study of the nutrition label approach. Retrieved from https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf
- [8]. Kim, G., & Koo, H. (2016). Full length article: The causal relationship between risk and trust in the online marketplace: A bidirectional perspective. *Computers in Human Behavior*, 55(B), 1020-1029. doi:10.1016/j.chb.2015.11.005

- [9]. Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *The Journal of Computer Information Systems*, 62–71.
- [10]. Motiwalla, L., Li, X., & Liu, X. (2014). Privacy paradox: Does stated privacy concerns translates into the valuation of personal information? PACIS 2014 Proceedings, 281. Retrieved from <http://aisel.aisnet.org/pacis2014/281>
- [11]. Norman, G., Pepall, L., Richards, D., & Tan, L. (2016). Competition and consumer data: The good, the bad, and the ugly. *Research in Economics*, 70, 752-765. doi:10.1016/j.rie.2016.09.002
- [12]. Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, 82, 331-338. doi:10.1016/j.jretai.2006.08.006
- [13]. Zhu, H., Ou, C. X., van den Heuvel, W., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, 54, 427-437. doi:10.1016/j.im.2016.10.001

David Cross " The Relationship between Privacy Notice Formats and Consumer Disclosure Decisions: A Quantitative Study" *International Journal of Business and Management Invention (IJBMI)*, vol. 09(03), 2020, pp 36-40.