"Inflicting pain for gain: Insights on the spam problem"

| AUTHORS | Ramendra Thakur
John H. Summey
Siva K. Balasubramanian
Arifin Angriawan |

NUMBER OF REFERENCES

0

NUMBER OF FIGURES

0

NUMBER OF TABLES

0

BUSINESS PERSPECTIVES

businessperspectives.org

Ramendra Thakur (USA), John H. Summey (USA), Siva K. Balasubramanian (USA), Arifin Angriawan (USA)

Inflicting pain for gain: insights on the spam problem

Abstract

Spam – or unsolicited commercial email – is a widespread problem. This study focuses on the implications of spam through the lens of marketing. We develop a model framework that draws on economic theory and regulatory literature to depict perceptions about cost effectiveness and government control as the drivers of customers' perceived spam intensity, with privacy invasion as the outcome. The framework is empirically tested using a partial least square (PLS) methodology. Results indicate that cost effectiveness is a significant predictor of consumers' perceptions of spam intensity while government policy is not. Government policy, however, has a negative influence on recipients' perception of privacy invasion. We discuss related implications for firms, consumers, public policy and future research.

Keywords: perceived spam intensity, government policy, cost effectiveness, customers' privacy invasion, e-commerce.

Introduction

"If the Internet could be removed, then spamming would disappear. But the problem is that we can not take away the Internet! What, therefore, do we do about the spam problem?"

David Wall (2004, p. 319)

Spam emails are a pervasive and growing problem. They are sent in bulk by some firms (often unscrupulous, anonymous, and therefore, seldom accountable) to sell a variety of goods and services. An email message is generally considered spam when it is received by a large number of recipients without prior consent. Research suggests that approximately 60 percent of Internet traffic is accounted for by spam (Nettleton, 2005). Therefore, there is a pressing need to enhance our understanding of the antecedents and consequences of the spam phenomenon.

Although the Internet is widely considered a beneficial resource, it remains a mixed blessing on the email frontier. Motivated by commercial gain, the practice of sending unsolicited bulk emails has expanded exponentially. Results from a 2005 survey conducted by the Center for Excellence in Service at the University of Maryland shed some light on potential reasons for this growth. They indicated that 11% of users purchased products and services in response to spam emails, despite the fact that 9% had previously lost money in email scams. A large group (39% of users) acknowledged clicking on embedded links within spam messages (other than the unsubscribe link) that alerts spammers that the email address is active, thereby triggering more spam, and potential exposure to computer viruses and spyware. These results are surprising especially because most recipients profess to hate spam.

Although spam is a key problem issue in ecommerce, scholars are yet to explore why businesses use the Internet for spamming, especially in light of negative outcomes generated among recipients (Sipior, Ward, and Bonner, 2004).

In theory, government policy may control and regulate spam. With respect to such policy, the following questions are of research interest. First, does governmental policy toward spam effectively reduce perceived spam intensity? Does governmental policy toward spam comfort consumers in any manner e.g., lower perceptions of privacy invasion? Does perceived spam intensity contribute to perceived privacy invasion?

We develop a structural model that depicts these and other relationships, reflecting theories drawn from economics and the literature on advertising regulation. We employ the partial least square (PLS) methodology to empirically validate the model and its hypotheses.

We organize this paper as follows. First, we briefly review the literature on two germane theories: economics and advertising regulation. Related theoretical rationales form the bases for hypotheses underlying our model framework. The second section empirically tests and validates the model and its hypotheses, and presents related results. The final section discusses findings, explores managerial implications, summarizes limitations, and offers suggestions for future research.

1. Literature review

1.1. Economic theory. Email is an expedient way to communicate a message. Emails are great communication vehicles because they are cost-effective and efficient. Unfortunately, email messages are exploited by some businesses to disseminate spam to customers regardless of their reluctance to receive such messages (Park and Deshpande, 2006). The cost involved in sending spam is negligible to the sender; the receiver and carriers – Internet Service Providers or ISP's – are forced to bear this burden (Park and Deshpande,

2006). Consistent with economic theory, this negligible cost is an incentive for firms to abuse the email medium to their advantage.

According to a Federal Trade Commission (FTC, 2003) report, the objectives of sending spam include:

♦ advertising or selling commercial products;

♦ sending pornographic materials;

♦ promoting get-rich and credit/financial schemes;

♦ selling health products.

Postini's (2006) study indicated that 28% of spam messages worldwide are related to discounted software, drugs, and herbal alternatives; respectively, 27%, 20%, 15%, and 10% of spam messages were related to frauds and scams, special offers, pornography, and other categories.

The Internet is misused as an e-medium because it is a relatively inexpensive way to reach large audiences (Marchewka, Liu, and Petersen, 2004). Prior studies argue that the email medium is attractive to spammers because email campaigns are 20 times less expensive than comparable direct mail campaigns (Disabatino, 2008). Economic theory suggests that the negligible cost of sending spam is the key reason why spam persists, especially in an environment where ISPs are unable to discourage businesses from abusing emails to promote or advertise products.

1.2. Theoretical perspectives on advertising regulation. Two theoretical/conceptual perspectives are evident in the literature on advertising regulation. First, advertising regulation broadly seeks to avoid unfair or deceptive messages, although this approach has to be balanced with freedom of speech. Scholars (e.g., Rotfeld, 1982) have appraised the compatibility of such regulation with the First Amendment's protection of free speech. The generally accepted consensus is that "advertising is entitled to First Amendment protection, but a lesser degree of protection than that provided for what is labeled as noncommercial speech" (Rotfeld, 1982, p. 139). Second, researchers have examined the pros and cons of government regulation and industry-based self-regulation. LaBarbera (1980) assessed the self-regulatory system and recommended greater public awareness and involvement. LaBarbera (1982)

found that acknowledging a commitment to self-regulation or government-regulation increased the persuasiveness of an advertiser with no prior reputation. Overall, the received wisdom from the literature points to the desirability of a combination of both industry-based self-regulation and government-regulation.

What are the implications of the preceding discussion for spam? First, spam messages generally do not suffer from deception or unfairness issues with regard to content *per se* that typically encourages advertising regulation. Second, the key concern about spam is the lack of good faith allegiance to consumer privacy and preferences. Third, self-regulation appears to have limited purview in the spam context because this approach only works if both the industry and the firm have reputations to protect. Spammers generally do not have great reputations or track records that need protection. The preceding discussion points to the need for empirical testing the impact of consumers' perceptions of regulation on their perceptions of spam prevalence, a task addressed in this study. Previous research indicates that both businesses and customers are increasingly fearful about invasion of their privacy due to spam (Nicolle, 2005). According to a recent study, customers believed that abusive emails involving commercial products, pornographic materials, and credit/financial schemes (directed at recipients who did not choose to have a relationship with the sender) should be controlled by Internet marketers (i.e., self-control), ISP intervention, or the government in order to ensure recipients' privacy (Marchewka, Liu, and Peterson, 2003).

2. Model derivation and hypotheses

Based on economic theory and the literature on advertising regulation, we derived the research model presented in Figure 1. Testable hypotheses from this model focus on four research questions that examine recipients' perceptions about spam: (1) Is cost effectiveness perceived to be a contributor of perceived spam intensity? (2) Does government policy have an impact on spam intensity? (3) Does consumers' perception of spam intensity lead to concomitant privacy invasion? and (4) Does government policy reduce perceptions of customers' privacy invasion?
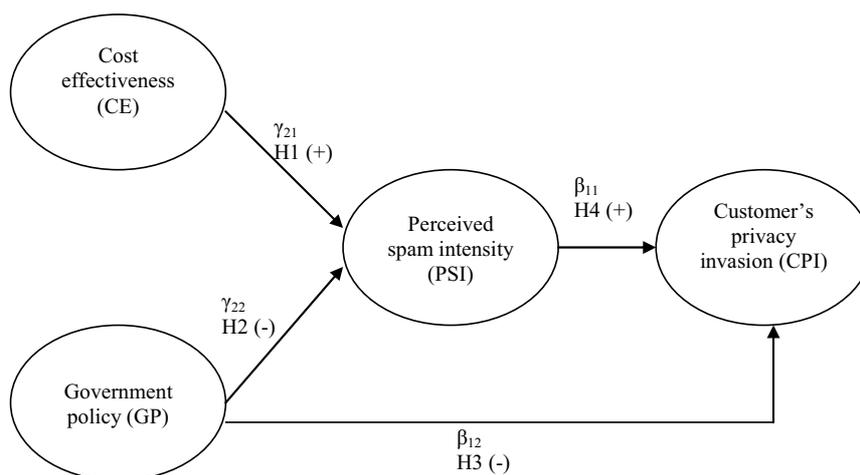
Fig. 1. Theoretical model

2.1. Cost effectiveness role. Watkins (2004) found a strong relationship between cost effectiveness and the amount of spam received by consumers. That study highlighted the low cost of sending unsolicited commercial emails as a key reason for the spam phenomenon. Another study by Customer Inter@ction Solutions in 2001 found cost as a motivator for their misuse in spamming. In our study, *cost effectiveness* is defined as cost-related motivation for spamming. Cerf's (2005) study indicated that businesses use email to spam because the only cost involved is the price paid for Internet connectivity.

There are indirect (and sometimes direct) costs to message recipients when they are forced to sort through voluminous spam (Zhang 2005; Schwartz and Garfinkel, 1998). Recent research by France (2002) suggests that spam is a cheap way to promote goods and services for firms intent on passing this cost to customers. Overall, the low cost in reaching customers has resulted in the misuse of this e-medium. We therefore posit:

H1: The more the businesses perceive the Internet to be cost effective (CE) in sending spam, the greater the spam intensity perceived (PSI) by customers.

2.2. Government policy role. Pressure from government, service providers, anti-spam activists and agitated customers has made life difficult for spam operators (Wood, 1999). Studies suggest that strict government policies against spammers may reduce the volume of junk mail from spammers (Ouellette, 1999). Government policy is a subjective concept relative to the strictness with which laws are enforced against spammers, especially on penalties imposed for violations.

When enforced effectively, government policy has yielded some reduction in spam volume. Strict legislation against spammers and effective enforcement may help Internet Service Providers (ISPs) and in-

dividuals combat spam (Wood, 1999). Strict government policy against abusive telephone sales programs, for example, increased consumers' trust in the "do not call list" program directed at telemarketers. The popularity of the DNC list reduced telemarketing abuse (Pour, 2004). Similar regulation against spammers has reduced perceptions of privacy invasion among customers (Pour, 2004).

To date, studies show that the CAN-SPAM act of 2003 (that took effect on January 1, 2004) has decreased spam volume directed at customers without their consent (Campbell 2004; Lee, 2005). We therefore hypothesize:

H2: The more stringent the government policy (GP) toward spam, the less the abuse of emails for spamming; therefore, the lower the spam intensity perceived (PSI) by customers.

H3: The more stringent the government policy (GP) toward spam, the lower the perceived invasion of customers' privacy (CPI).

2.3. Customer's privacy invasion role. Customers' concerns about privacy invasion discourage acceptance of Internet technology (Nobel and Callaghan, 2000). In their study, customers' privacy invasion was defined as intrusion into the customer's domain without their acquiescence (this reflects the spirit of the argument advanced by Warren and Brandies (1890) – see Chung (2002)). According to Rogers (2004), spam is considered an affront to personal privacy.

Consistent with Garee and Schori (1997) and Zorkadis et al. (2005), we view spamming an invasion of customer's privacy. The most troubling types of unsolicited mails have been identified as get-rich-schemes, adult pornographic site promotions, and ads for pharmaceutical products such as Viagra. Spammers rely on the Internet to heavily advertise their products/services because of the minimal cost involved for sending bulk emails.

Indirectly the cost gets shifted from the spammers to recipients and other parties such as Internet Service Provider's (ISPs) or organizations where recipients work (because deleting unwanted spam messages entails costs). Studies show that spam clogs customers' email inboxes that represent their personal space and privacy (Marks, 2004). Hence, we hypothesize that:

H4: As perceptions of spam intensity (PSI) increases, customers' perception of privacy invasion (CPI) also increases.

3. Methodology

Informants for our survey research represent a probability sample of faculty, staff, and instructors from a major Midwestern university. We selected this pool of subjects because: (1) they represent a broad spectrum of income groups; and (2) we sought to understand the perceptions of this group of consumers about the amount of spam they receive.

Prior to administering the survey, the questionnaire was pre-tested and revised to ensure readability and a logical arrangement of questions. The final sample included 177 respondents (71 males and 106 females), the majority of whom were between 35 and 64 years old (73.6%).

Subjects were highly educated: 5.1% had professional degrees (Ph.D., MD, etc.), 22.7% had a Master's degree, and approximately 29% had an undergraduate education. About 83% were white, while the remaining belonged to the following ethnic categories: African American, Asian American or Hispanic. About 41% reported annual income above $50,000; 42% had an income between $25,000 and $49,999. Table 1 summarizes demographic profile of informants.

Table 1. Demographic profile

Demographic	Frequency, %
Gender	
Male	71-40.1
Female	106- 59.9
Age	
18 to 24 years	10-5.6
25 to 34 years	34-19.1
35 to 44 years	38-21.3
45 to 54 years	51-28.7
55 to 64 years	42-23.6
65 years and above	3-1.7
Education	
Grammar school	1-0.6
High school	13-7.4
Vocational school	19-10.8
College graduate	51-29.0
Master's degree	40-22.7
Postsecondary degree (PhD, MD, etc.)	43-24.4
Others	9- 5.1

Ethnicity	
Caucasian	147-82.6
Black/African American	17-9.6
Asian, Pacific Islander	5-2.8
Hispanic	1-0.6
American Indian	2-1.1
Decline to answer	6-3.4
Profession	
Administrative profession	36-20.2
Faculty member	48-27.0
Administrative staff	77-43.3
Students (Graduate/Undergraduate)	17-9.6
Income	
Under $9,999	4-2.4
$10,000 to $24,999	28-16.5
$25,000 to $49,999	71-41.8
$50,000 to $74,999	40-23.5
$75,000 to $99,999	10-5.9
Over $100,000	17-10.0

3.1. Measurement of constructs in model. The items to measure the four model constructs were either adapted from previous research or created specifically for this study (all measurement items used are listed in the Appendix). All items sought responses on a 7-point scale ranging from 1 (strongly disagree) to 7 (strongly agree).

3.2. Model specifications and analysis. Our theory and hypotheses suggest the following model of spam and its consequences (see Fig. 1):

Customer Privacy Invasion $= \beta_{11}$ (Perceived Spam Intensity) $+ \beta_{12}$ (Government Policy) $+ \varepsilon_1$;

Perceived Spam Intensity $= \gamma_{21}$ (Cost Effectiveness) $+ \gamma_{22}$ (Government Policy) $+ \varepsilon_2$.

This model was tested using partial least square (PLS) approach, using PLS-Graph (version 3.00, build 1126) software. As suggested by Sundaram et al. (2007) and Chin and Newstead (1999), we chose the PLS approach over the popular two-step covariance-based approach to model estimation (Anderson and Gerbing, 1982; Gerbing and Anderson, 1985) because the former is appropriate for the relatively small sample size (n = 177) in our study.

4. Results

The measurement model was first estimated and then the structural model was tested. Since our study advances directional hypotheses, we use the one-tailed significance test for testing them (Chandy and Tellis, 1998).

4.1. Measurement model. To assure reliability and validity of the measured variables, we used a measurement model where the 14 measurement items were linked to each of the four proposed constructs. The purpose of this commonly used approach is to ascertain that each measurement item only loads on its respective underlying latent construct, as described in an earlier section. The standardized load-

ings of the variables measuring the underlying constructs ranged from 0.727 to 0.951, thereby meeting the unidimentionality threshold of 0.70 (Chin, 1998). As suggested by Sundaram et al. (2007), cross-loadings were computed to determine if the items loaded only on their underlying constructs or on other constructs as well. Results show that none of the items loaded higher on any other construct than on their underlying constructs.

Table 2. Loadings and cross-loadings

	Cost effective-ness	Government Policy	Perceived Spam Intensity	Customer Privacy Invasion
CE1	0.8521	-0.2272	0.2509	0.3322
CE2	0.8728	-0.2171	0.1815	0.2740
CE3	0.8451	-0.1896	0.2542	0.1924
GP1	-0.2842	0.9039	-0.0023	-0.3497
GP3	-0.1953	0.8759	-0.0512	-0.3059
R_GP4	-0.0817	0.7267	0.0182	-0.1569
PSI1	0.1736	-0.0191	0.8312	0.1464
PSI2	0.2481	0.0180	0.7534	0.1809
PSI3	0.1523	-0.0448	0.8412	0.2169
PSI4	0.1934	-0.0697	0.8032	0.2145
PSI7	0.2982	0.0180	0.8295	0.2014
CPI1	0.3172	-0.3016	0.2698	0.9322
CPI2	0.3006	-0.3398	0.2278	0.9509
CPI3	0.2302	-0.3093	0.1521	0.8722

Notes: Numbers in bold are item loadings on their underlying constructs. Other numbers are the cross-loadings. To calculate cross-loadings first we calculated the latent variable scores (provided by PLS-Graph) and standardized indicator scores for each construct. Then we correlated latent variable scores and standardized indicator scores to calculate cross-loadings. Numbers in the bold should be greater than cross-loadings (Sundaram, Schwarz, Jones and Chin, 2007).

After establishing undimensionality and cross-loadings, we assessed Cronbach's alpha and composite reliabilities. We also used the Multitrait-Multimethod Matrix (MTMM) approach (Campbell and Fiske, 1959) that relies on convergent and discriminant validities to support the model validation process (see Table 3).

Convergent validity helps ensure that concepts that *should* be related theoretically are *actually* interrelated in reality. Discriminant validity conveys the degree to which concepts that should *not* be related theoretically are, in fact, *not* interrelated in reality (Campbell and Fiske, 1959). According to Fornel and Lacker (1981a; 1981b), convergent validity is supported if the average variance extracted (AVE) estimates exceed 0.50. Similarly, discriminant validity is established when the shared variance between any two constructs is less than the square root of the AVE by the items measuring the construct.

Table 3. Interconstruct correlations

	Cronbach alpha	Composite reliability	Average variance extracted	CE	GP	PSI	CPI
Cost effectiveness (CE)	0.810	0.892	0.734	0.857			
Government policy (GP)	0.795	0.876	0.704	-0.246	0.839		
Perceived spam intensity (PSI)	0.873	0.906	0.660	0.273	-0.020	0.812	
Consumer privacy invasion (CPI)	0.904	0.942	0.845	0.310	-0.345	0.239	0.919

Note: Diagonal elements represent the square root of the average variance extracted (AVE) between the constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements.

4.2. Structural model. The structural model tested four hypothesized paths between the four latent constructs. A path is considered significant if the *t*-value associated with the path is greater than 1.64. The results of the structural model using PLS Graph are shown in Figure 2 and Table 4.

Of the four paths tested, three paths were statistically significant at 0.001 level. A direct path from cost effectiveness (H1) (b = 0.286, p < 0.001) to perceived spam intensity is positive and statistically

significant. However, a direct path from government policy (H2) to perceived spam intensity was found to be non-significant. Thus hypothesis H1 was supported while H2 was not. The PLS results also show that the direct path from government policy (H3) (b = -0.340, p < 0.001) has a negative relationship with customers privacy invasion, thereby supporting H3. As predicted in H4, perceived spam intensity was found to be a statistically significant and positive driver of customer's privacy invasion, with a parameter estimate of 0.232.
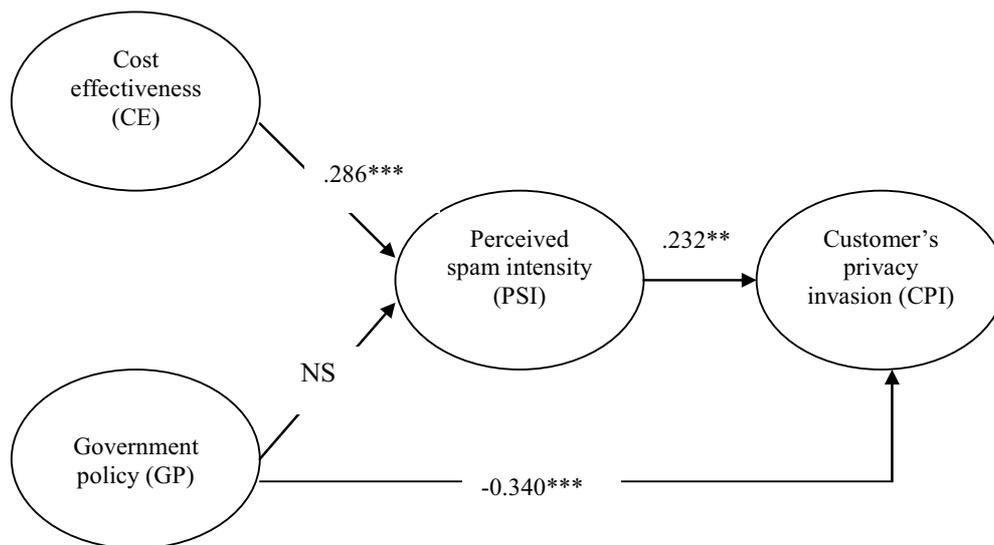
Note: ** p < 0.01; *** p < 0.001. NS = non-significant.

Fig. 2. Final model

Table 4. Standardized path coefficient and *t*-value for the structural model

Parameter estimates structural paths	Standardized path coefficients	t-value	Hypotheses supported
H1: CE -> PSI	0.286	3.599***	Yes
H2: GP -> PSI	0.051	0.691	No
H3: GP -> CPI	-0.340	6.090***	Yes
H4: PSI -> CPI	0.232	2.442**	Yes

Note: ** p < 0.01; *** p < 0.001. CE = Cost effectiveness; GP = Government policy; PSI = Perceived spam intensity; CPI = Customer's privacy invasion.

Discussion

Prior research has focused on factors that encourage businesses toward spam. Our research broadly supports this premise. In addition, our study documents the following: (1) spam infringes customers' perception of privacy; and (2) generates negative attitudes toward emails in general and toward spammer firms in particular. Ultimately, customers' perceptions about privacy invasion due to spam restrict the creation of value networks or relationships between the customer and the firm involved. To our knowledge, this is the first empirical study to examine key predictors of spam from the recipients' perspective. Our research also addresses the impact of spam on recipients' perceptions of privacy invasion.

This study provided evidence that, of the two exogenous constructs (cost effectiveness and government policy) considered, only cost effectiveness is a significant predictor of perceived spam intensity. This could be because informants perceive loopholes in government policies that spammers often depend upon to gain advantage.

Two model constructs (government policy and perceived spam intensity) were found to be significant predictors of customers' perceptions of privacy invasion. The path coefficient from these two constructs to customers' privacy invasion indicated that government policy was a strong predictor of perceptions of privacy invasion, whereas perceived spam intensity was found to be positively related to customer's privacy invasion. Overall, the individual path estimates for the model provide support for three out of four hypotheses tested for statistical significance.

The Internet provides a "free ride" to spammers, thereby encouraging misuse of this medium with unsolicited commercial emails. Informants appear to perceive that the low cost of sending unsolicited commercial emails motivates some firms to indulge in spamming behavior. Although the immediate burden of this falls on the Internet service provider's (ISP's) and email recipients, it is unfortunate that legitimate firms that desire to use emails for building customer relationships have to suffer some of the negative consequences as well.

Our study reinforces customers' perceptions that firms find emails are cost-effective for promoting products, and that this in turn encourages spamming. Marchewka et al. (2004) found that

sending bulk emails was so cost effective when compared to other traditional marketing medium that there was little incentive for businesses to target emails to individual customers. Significant negative aftermath of spam include the feeling of insecurity and invasion of privacy. Such insecurity inhibits customers' interest in building relationships with firms, and may eventually inhibit the creation of value networks between firms and customers.

The building of relationships between firms and customers, rather than simply enabling transactional exchanges, is based on trust. A strict government policy against spammers could enhance consumers' trust in e-media, increase willingness to use the services of firms that use it, and strengthen relationships between customers and firms.

Managerial implications, limitations, and future research

The primary contribution of this research is to enhance our understanding of factors that encourage firms toward spam. Unsolicited commercial emails that attempt to sell services and goods generate negative impact on relationship building and value creation efforts involving firms and customers. Our investigation also addresses two related questions: Does spam infringe customers' privacy? Are government policies perceived to impact spam?

Results show that if a business wants to build customer relationships, it should not send unsolicited emails. Unfortunately, most customers may perceive spam as invasion of their privacy. Second, misuse of email for spamming not only reduces the value of the electronic medium per se; it also makes customers feel insecure.

This research is subject to the limitations discussed next, some of which also represent opportunities for future research. First, it is desirable that applications of structural equation modeling approach should document results using a calibration sample and a validation sample. Unfortunately, the relatively small sample size of this study precluded this approach to validation, a task that could be addressed in future research. A future replication study of this kind will help to verify and validate our findings. Another possible opportunity is to try to replicate the findings of this study in different countries to understand the attitude of respondents about spam.

Studies could also be carried out to examine factors other than those discussed in this study that could serve as predictors of spam. For example, research should be carried out to see the impact of factors like customer's willingness to receive promotions and the normative codes of conduct that firms should follow with regard to spam.

References

1. Anderson, J.C., D.W. Gerbing. Some methods for respecifying measurement models to obtain unidimensional construct measure // *Journal of Marketing Research*, 1982. – No 19. – pp. 453-460.
2. Campbell, M. Canning spam // *Entrepreneur*, 2004. – No. 32. – pp. 39-40.
3. Campbell, D.T., D.W. Fiske. Convergent and discriminant validation by the multitrait multimethod matrix // *Psychological Bulletin*, 1959. – No. 56. – pp. 81-105.
4. Cerf, V.G. Spam, spim, and spit // *Communications of the ACM*, 2005. – No. 48. – pp. 39-43.
5. Chandy, R.K., G.J. Tellis. Organizing for radical product innovation: The overlooked role of willingness to cannibalize // *Journal of Marketing Research*, 1998. – No. 35. – pp. 474-487.
6. Chung, W. A soop at privacy issue on the internet in New Zealand. University of Auckland // *Business Review*, 2002. – No. 4. – pp. 2-15.
7. Chin, W.W., P.R. Newsted. Structural equation modeling analysis with small samples using partial least squares. In R. Hoyle (ed.), Statistical strategies for small sample research, Thousand Oaks, Sage: CA, 1999. – pp. 307-341.
8. _____. The partial least squares approach for structural equation modeling. In G.A. Marcoulides (ed.), Modern Method for Business Research, Marwah, Erlbaum: NJ, 1998. – pp. 295-336.
9. Customer Inter@ction Solutions. E-mail Management Technologies Roundup. 2001. – No. 19. – pp. 58-60.
10. Disabatino, J. Online Marketers Stung by Spam Label. Computerworld, November 2, 2000. Available online: www.computerworld.com/printthis/2000/0,4814,543480,00.html, accessed on: July 2, 2008.
11. Fornell, C., D.F. Larcker. Structural equation models with unobservable variables and measurement error: Algebra and statistics // *Journal of Marketing Research*, 1981. – No. 18. – pp. 382-388.
12. _____, _____. Evaluating structural equation models with unobservable variables and measurement error // *Journal of Marketing Research*, 1981. – No. 18. – pp. 39-50.
13. France, M. Needed now: Laws to can spam // *Business Week Online*, 9/27/2002, available online: http://www.businessweek.com/smallbiz/content/sep2002/sb20020926_5958.htm, accessed on: July 2, 2008.
14. Garee, M.L., T.R. Schori. Is 'spamming' an invasion of privacy or high-tech 'direct mail'? // *Marketing News*, 1997. – No. 31. – pp. 4.
15. Gerbing, D.W., J.C. Anderson. The effects of sampling error and model characteristics on parameter estimation for maximum likelihood confirmatory factor analysis // *Multivariate Behavioral Research*, 1985. – No. 20. – pp. 255-271.
16. Hair, J.F., R.E. Anderson, R.L. Tatham, W.C. Black. Multivariate Data Analysis, 5th ed., Prentice Hall, New Jersey, 1998.

17. LaBarbera, P. Advertising self-regulation: An evaluation // *MSU Business Topics*, 1980. – No. 28. – pp. 55-63.
18. _____. Overcoming a no-reputation liability through documentation and advertising regulation // *Journal of Marketing Research*, 1982. – No. 19. – pp. 223-228.
19. Lee, Y. The CAN-SPAM act: A silver bullet solution? // *Communications of the ACM*, 2005. –No. 48. – pp. 131-132.
20. Marchewka, J.T., C. Liu, C.G. Peterson. Issues and perceptions of unsolicited commercial electronic mails // chapter in the book The social and cognitive impact of e-Commerce on modern organizations, Idea Group Publishing, 2004.
21. Marks, E.E. Spammers clog in-boxes everywhere: Will the CAN-SPAM act of 2003 halt the invasion? // *Case Western Reserve Law* Review, 2004. – No. 54. – pp. 943-963.
22. Nettleton, E. Getting tough on spam? // *Journal of Database* Marketing *& Customer Strategy Management*, 2005. – No. 12. – pp. 357-361.
23. Nicolle, L. Open the door to a secure career // *Computer Weekly*, 2/8/2005. – pp. 28-29.
24. Nobel, C., D. Callaghan. Wireless services hit snags // *eWeek*, 2000. – No. 17.
25. Ouellette, T. Spam // *Computerworld*, 4/5/99, – No. 33. – pp. 70.
26. Park, J.S., A. Deshpande. Spam detection: Increasing accuracy with a hybrid solution // *Information Systems Management*, 2006. – No. 23. – pp. 57-67.
27. Postini. Spam messages worldwide, by type, 2005 (% of Total), available at: www.eMarketer.com, January 2006.
28. Pour-Mehdi, K. The social and cognitive impact of e-Commerce on modern organizations, Idea Group Publishing, 2004.
29. Rogers, K.M. The privacy directive and resultant regulations – The effect on spam and cookies // Part I, *Business Law Review*, 2004. – No. 25. – pp. 271-274.
30. Rotfeld, H.J. The compatibility of advertising regulation and the first amendment – another view // *Journal of Public Policy & Marketing*, 1982. – No. 1. – pp. 136-146.
31. Schwartz, A., S. Garfinkel. Stopping spam, Pub.: O'Reilly & Associates, CA, 1998.
32. Sipior, J.C., B.T. Ward, P.G. Bonner. Should spam be on the menu? // *Communication of the ACM*, 2004. – No. 47. – pp. 59-64.
33. Sundaram, S., A. Schwarz, E. Jones, W.W. Chin. Technology use on the front line: How information technology enhances individual performance // *Journal of the Academy of Marketing Science*, 2007. – No. 35. – pp. 101-112.
34. Wall, D.S. Digital realism and the governance of spam as cybercrime // *European Journal of Criminal Policy and Research*, 2004. – No. 10. – pp. 309-355.
35. Watkins, E. The hidden costs of technology // *Lodging Hospitality*, 2004. – No. 60. – p. 2.
36. Warren, S., L. Brandeis. The Right to Privacy // *Harvard Law Review*, 1980. – No. 4.
37. Wood, D. Programming Internet Email, Pub: O'Reilly & Associates, CA, 1999.
38. Zhang, L. (2005). The Can-Spam act: An insufficient response to the growing spam problem // *Berkeley Technology Law Journal*, Annual Review 20. – pp. 301-322.
39. Zorkadis, V., D.A. Karras, M. Panayotou (2005). Efficient information theoretic strategies for classifier combination, feature extraction and performance evaluation in improving false positives and false negatives for spam e-mail filtering // *Neural Networks*. – No. 18. – pp. 799-807.

Appendix

Items used to operationalize constructs

Perceived spam intensity (7-point scales anchored by strongly disagree and strongly agree). A message is considered to be a spam if:

S1   The message is deceptive.
S2   Sender is unknown.
S3   Subjective matter is offensive.
S4   Subjective heading is unfamiliar.
S7   It is a chain letter.

Cost effectiveness (7-point scales anchored by strongly disagree and strongly agree):

CE1   The Internet provides a "free ride" to the spammer.
CE2   Low cost has attracted abusers to send spam.
CE3   It is cheap to send spam.

Government policy (7-point scales anchored by strongly disagree and strongly agree):

GP1   Strict government policy would have a positive impact on decreasing the number of spam messages.
GP2   Harsh penalties on spammers would reduce spamming.
GP3   Government policy on spam would have little or no impact on spammers (reverse coded).

Customer's privacy invasion (7-point scales anchored by strongly disagree and strongly agree):

CPI 1   Spam invades people's personal space.
CPI 2   Spam is an infringement of people's privacy.
CPI 3   Spam is a violation of people's right to choose what they use an Internet connection for.