

An Analytical Paper on Privacy issues of Consumers in Unsolicited marketing campaign

Dr .A. IRIN SUTHA
Assistant Professor
Department of Commerce
Faculty of Science and Humanities
SRM University

Mr. J.Solomon Thangadurai
Research Scholar
Department of Commerce
Madras Christian College
East Tambaram Chennai -600059
M: 9884738036
E:solomonthangadurai@gmail.com

Abstract:

E-commerce privacy being an vital issue that has been resulting in negative or adverse effects on the additional development and growth of e-commerce. With the speedy growth and use of E-commerce, privacy has become associate degree in progress and increasing concern for the users, providers, applied scientist still because the policy manufacturers. whereas it's tough to finish a dealing in e-commerce by a user while not providing personal data, protective that data from proliferating is another tough issue for the suppliers, applied scientist and also the policy manufacturers. Psychologically, users' of e-commerce are unwilling to produce personal data or perhaps to browse on-line if they believe their privacy isn't protected. As luck would have it, there are technologies still as policies are in impact, still as are in development stages to assist shield privacy at current and in future. TRUSTe, BBBonline and WebTrust are a number of

the businesses providing services for standardized privacy protection technology and policy. However, there's a necessity to grasp a lot of concerning the vary of privacy problems so as to make usable and effective mechanisms for those firms and different privacy protection technologies and policies. This paper presents previous, existing and future privacy problems and their solutions in respect privacy concern in unsolicited marketing campaign.

Keywords: Applied scientist, policy manufacturers, proliferating, unsolicited

[I] Introduction:

In the early years of this market that the convenience with that e-mail address collected for nothing and therefore the low overall value of in operation would attract amateur operators who cared nothing for the Internet's rule and therefore the privacy of its users. The last half of the 90s was marked by associate degree explosion within the development notable by that ugly word

“spam”.

The world of spam in e-mail promoting, it contains a close discussion of spamware – software system packages that may be accustomed harvest e-mail addresses within the Internet’s public areas – and therefore the legal and money risks currently facing those that use them.

E-mail promoting has been characterized by some rather crude practices, in line with the definition given by the CNIL, spam “(...) is that the bulk-mailing, generally repeatedly, of uninvited e-mail messages, sometimes of an ad nature, to people with whom the mailer has had no previous contact and whose email addresses the mailer collected from the general public areas of the Internet: newsgroups, mailing lists, directories, internet sites etc.”. Spam has skilled variety of stages; however because of a strong backlash by web activist’s opposition the development of the net, pressure from privacy advocates and action by legislators, it's currently in retreat or a minimum of evolving into less unacceptable forms.

In the last decade the continual growth of the spam development, particularly the majority delivery of unsought e-mails, primarily of economic nature, however additionally with offensive content or with fallacious aims, has become a main drawback of the e-mail service for web service suppliers (ISP), company and personal users. Recent surveys report says that over 60% of e-mail traffic is spam. Spam causes e-mail Systems to expertise overloads in information measure and server storage capability, with a rise in annual price for companies of over tens of billions of dollars. Additionally, phish-ing spam emails are a heavy threat for the safety of finish

users, since they fight to convert them to surrender personal data like passwords and account numbers, through the utilization of spoof messages that are masqueraded as returning from prestigious on-line businesses like money establishments.

In e-commerce usually needs the revealing of enormous amounts of private information. Necessary information includes credit card information and delivery details. Additionally the possession of such information offers e-business the chance to investigate it, discovering trends and increasing the potency of their business dealings. Customers usually had no plan on the vary of attainable uses that possession of this information permits for, and therefore had no plan on the attainable violation of their privacy that would occur M.Q.Fang 1999¹

Scam: As on-line searching is turning into quite common the amount of on-line scam and fraud is additionally increasing. This is often why a customer must always purchase from trustworthy websites solely as a result of trustworthy websites would pay attention of any fraud to keep up their name.

Be aware of email scams designed to half you from your credit card data.

Email frauds that square measure designed to collect personal data like passwords and master card details square measure called phishing emails. The thought is that thousands or many thousands square measure sent enter the hope of reeling in unsuspecting victims and obtaining them to

give wind. The emails seem to be from well-known firms and may look quite convincing. However, legitimate firms, as well as all banks, can never send you Associate in nursing email with a link requesting your login, password, or master card details. If unsure, kind the online address of the corporate it relates to directly into the browser instead of following the e-mail link.

Opt - In VS. Spam Technique:

Before beginning e-mail promoting campaign, the marketers ought to clearly perceive the distinction between opt-in e-mail promoting and spam. If they fail to try that, they'll hurt the business and their name for an extended time. (Barnes and Scornavacca, 2004)⁵. Spam could be a terribly unethical manner of web promoting. merely explicit , it suggests that causation promotional e-mail messages to those that failed to request for them. If the trafficker tries to send unplanned e-mails or spam, the ISP (Internet Service Provider) might ban these e-mails and can ne'er be ready to send messages from your e-mail account once more. Opt-in e-mail promoting is healthier than spamming. Opt-in is totally different from the spam; since it's permission primarily based, which implies that folks have united to receive e-mails from you (Sullivan and DeLeeuw, 2003⁶; Barnes and Scornavacca, 2004). In several businesses, marketers square measure most well-liked to plug this manner because it brings superb results (Alam, 2010)⁷. a number of the highest marketers have achieved four-hundredth response rates victimization opt-in

E-mail promoting. An extra advantage of opt-in over spam technique is that:

1. Spam brings terribly low response rates

2. it's not targeted, which implies that e-mail message goes to anybody, World Health Organization|those that|people who} have an interest in your provide and people who aren't.

The important part of the receivers would not even look at these e-mails and thus, reaching wonderful response rates using spam advertisement seem not possible. On the other side, opt-in technique is targeting the people who would love to receive the advertisements (that is, when the marketer sends a message to a listing of e-mail addresses, he or she knows the list is interested in the offer

[2] Review of Literature:

In the current globalized, data societies the increasing importance of privacy is been wide mentioned and is presently undisputed. Several researches and various works are conducted that helped the net shoppers to grasp the privacy in any respect the amount, individual structure and social (Heng Xu et.al, 2008)². Privacy as a plan is in disarray. No one will articulate what it suggests that. Apart kind that privacy has been delineate as multidimensional, elastic, relying upon context, and dynamic within the sense that it varies with life experience || (Heng Xu et.al, 2008). More on-line privacy issues (Dinev and Hart, 2004)³ square measure been involved as isolated efforts that square measure won't to establish and discuss the factors that influence the buyer privacy issues.

Reveal personal data on-line – here on-line shoppers refuse to reveal their personal data on web, therefore this leads to browsing websites wherever personal data is captured or needed or typically even false personal

data can be given to use the context (Dinev and Hart, 2004).

Enter into e-commerce transactions – this might lead shoppers to not use e portals for creating transactions intrinsically transactions would like revelation of sensitive personal data like communicating address, email, phone numbers etc. (Dinev and Hart, 2004)

Technology of security: Most of the participants did not show much interest in technology used for security. The log on pages is the first level of security and most of the people are aware of this. When the participants are checked for the knowledge of security systems they are unaware of them. Most of the participants know about the log on page and few claims to be familiar with SSL, https, and encryption. Many people feel that they have nothing to do with this, but some explain that encryption is for highest level of security offered by the web site (Cheskin Research, 1999)⁴.

[3] Objectives of the study:

1. To identify the consumer segment by analyzing respondents demographic characteristics
2. To know the consumer response towards unsolicited mails
3. To find the difference between Opt In and Spam
4. To identify the consumer privacy issues

5. To give suggestion to minimize the unsolicited spam and privacy issues prevailing among consumers

[4] Analysis and Interpretation:

Table: 4.1. Indicating Cronbach’s Alpha as reliability tool to validate the data:

Reliability Statistics	
Cronbach's Alpha	N of Items
.878	26

Interpretation:

The reliability for 26 items is 0.848. Even if one of the 25 items is deleted the Cronbach’s Alpha value will be reduced. This indicates that the reliability for all items is higher.

Frequency Table based on respondents Demographic Characteristics:

Table No: 4.2. Classification of respondent’s on the basis of Age

Age Group	Frequency	Percent	
Valid	18-25	29	29.0
	26-35	37	37.0
	36-45	28	28.0
	46-55	6	6.0
	Total	100	100.0

Interpretation:

The frequency table shows 37% of respondents are in 26-35 age group and 6% of respondents are in 46-55.

Table No: 4.3. Classification of respondent’s on the basis of Gender

Gender Group	Frequency	Percent
Valid Male	32	32.0
Valid Female	68	68.0
Total	100	100.0

Interpretation:

The frequency table shows 68% of respondents are Female and 32% respondents are Male.

Table No: 4.4. Classification of respondent’s on the basis of Monthly Income

Monthly Income	Frequency	Percent
Valid <10000	10	10.0
Valid 10000-20000	8	8.0
Valid 20001-30000	27	27.0
Valid 30001-40000	35	35.0
Valid 40001-50000	5	5.0
Valid >50000	15	15.0
Total	100	100.0

Interpretation:

The frequency table shows 35% of respondents have Rs. 30,001-40,000 monthly income and 5% respondents are belonging to 40,001-50,000.

Table No: 4.5. Classification of respondent’s on the basis of Occupation

Occupational Group	Frequency	Percent
Valid Government employees	7	7.0
Valid Private Employees	44	44.0
Valid Housewife	5	5.0
Valid Business	9	9.0
Valid Professional	4	4.0
Valid Part Time Jobs	1	1.0
Valid Student	30	30.0
Total	100	100.0

Interpretation:

The frequency table shows 44% of respondents are private employees, and 1% of respondents are in Part time jobs.

Table No: 4.6. Classification of respondent’s on the basis of Educational Qualification

Qualification Group	Frequency	Percent
Valid Graduate	15	15.0
Valid Post graduate	76	76.0
Valid Professional	9	9.0
Total	100	100.0

Interpretation:

The frequency table shows 76% of respondents are Post graduate and 9% of respondents are professional.

Frequency table on the basis of Consumer response towards unsolicited mail

Total	100	100.0
-------	-----	-------

Table No: 4.7. Respondent’s level of spam box checking:

Have you checked your spam box before		Frequency	Percent
Valid	Always	15	15.0
	Often	15	15.0
	Sometimes	29	29.0
	Rarely	27	27.0
	Never	14	14.0
	Total	100	100.0

Interpretation:

The frequency table shows 29% of respondents respond they check spam box sometimes and 14% of respondents respond they never check spam box

Table No: 4.8. Respondent’s level of awareness towards email considered as spam:

Do you know sometimes there are emails considered as spam but they are not?		Frequency	Percent
Valid	Neutral	5	5.0
	Agree	49	49.0
	Strongly Agree	46	46.0

Interpretation:

The frequency table shows 49% of respondents agree that they know emails sometimes considered as spam mail and 5% of respondent’s neutral with the statement.

Table No: 4.9. Respondent’s agreement with privacy issues statement:

Agreement with control Privacy Issues	Strongly Agree %
Consumers not interested in getting information from unfamiliar companies	13%
I would request company to remove information if misused	80%
Companies share information with other without permission	36%
Companies should have privacy protection policies	78%
Privacy protection policies should indicate how it will protect my information	74%
Consumer information is misused	37%
I receive too much advertising material	47%
I am pleased to receive information from unfamiliar companies	6%
Companies should have privacy protection policies indicating reasons for protection	70%
I am concerned about misuse	53%
Companies must have privacy protection policies	70%

I believe that companies use information for other purposes	38%
I feel uncomfortable when companies share information	70%
Companies regularly share information with others to offer products and services	39%
Government should limit companies' use of information	65%
I do not mind receiving telephone calls	3%
Companies send too much advertising material	41%
I refuse to provide personal information without reason supplied	65%
I would support a company's effort to ensure safety	63%
I fear that personal information may not be safe while stored	39%
Information is safe while stored in a company's records	3%
Government should do more to protect safety of information	61%
Too many companies call to sell products and services	60%
Government should restrict information collection	56%

Interpretation:

The above table shows respondents with privacy issues statement, most of the factors are above 50% strongly agreed by the respondent's consumers aware of privacy issues which are increasing every year. Table shows respondents have good opinion on company that they will restrict the spam mail and privacy issues.

[5] Conclusion:

Individuals who feel that they have been victims of privacy invasion will have higher concern and do more to actively protect their

information. Victims are generally those who refuse to provide their personal information notify companies not to send them advertising material and are not aware of name removal options. Those with high concern (the so-called Fundamentals) show active protective behavior, refuse to provide personal information, request removal of information and are not aware of name removal options.

According to Udo (2001)⁸ sites in which privacy concerns are sensitive should clearly display privacy policies and should offer the consumer to choose to share their personal information or restrict its use and such sites should also state how to use the privacy policies.

Unlike SMS marketing or other marketing services, e-mail marketing service is cheap, might reach millions of end users, and however anti-spam has become a real challenge for this kind of marketing. Few researches provide a wide study to evaluate the influence of anti-spam systems on the e-mail marketing service. A study case to evaluate the drawback of anti-spam effect on the e-mail marketing service has been presented in this paper.

Overall this study stresses on the importance implementing effective security and privacy policies thus on increase the patron trust. Therefore it's believed that such policies can increase client awareness on e portals, reducing risk and liabilities and this successively can develop trust in customers. In closing this study indicates that there's a necessity of security and privacy assurance and this responsibility must be haunted by the e merchants and/or vendors, government and will see that they provide assurance to its customers that their security and privacy is protected.

[6] Reference:

1. M. Q. Fang, “The Conspectus of E-Commerce,” Tsinghua University Press, Beijing, 1999
2. Heng Xu, Tamara Dinev, H. Jeff Smith and Paul Hart (2008), Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View, Association for Information Systems, Year 2008
3. Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model. *Behavior and Information Technology*, 23 (6), 413-422.
4. Cheskin Research / Sapient. E-Commerce trust study, January 1999.
5. Barnes SJ, Scornavacca E (2004). "Mobile marketing: the role of permission and acceptance." *Int. J. Mobile Comm.*, 2(2): 128-139.
6. Sullivan JD, DeLeeuw MB (2003). "Spam after Can-Spam: How Inconsistent Thinking Has Made a Hash out of Unsolicited Commercial E-Mail Policy." *Santa Clara Computer & High Tech. LJ* 20: 887.
7. Alam, GM., Hoque, KE (2010). Who gains from “Brain and Body Drain” Business -Developing/developed world or individuals: A comparative study between skilled and semi/unskilled emigrants, *Afr. J. Bus. Manage.*, 4(4): 534-548.
8. Udo, G. J. (2001). Privacy and Security Concern as Major Barrier for E-commerce: A Survey Study. *Information Management and Computer Security*, Vol.9, No. 4, pp 165-175.