International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Chief Patron

Dr. JOSE G. VARGAS-HERNANDEZ
Member of the National System of Researchers, Mexico
Research professor at University Center of Economic and Managerial Sciences, University of Guadalajara
Director of Mass Media at Ayuntamiento de Cd. Guzman
Ex. director of Centro de Capacitacion y Adiestramiento

Patron

Dr. Mohammad Reza Noruzi
PhD: Public Administration, Public Sector Policy Making Management, Tarbiat Modarres University, Tehran, Iran
Faculty of Economics and Management, Tarbiat Modarres University, Tehran, Iran
Young Researchers' Club Member, Islamic Azad University, Bonab, Iran

Chief Advisors

Dr. NAGENDRA. S.
Senior Asst. Professor,
Department of MBA, Mangalore Institute of Technology and Engineering, Moodabidri

Dr. SUNIL KUMAR MISHRA
Associate Professor,
Dronacharya College of Engineering, Gurgaon, INDIA

Mr. GARRY TAN WEI HAN
Lecturer and Chairperson (Centre for Business and Management),
Department of Marketing, University Tunku Abdul Rahman, MALAYSIA

MS. R. KAVITHA
Assistant Professor,
Aloysius Institute of Management and Information, Mangalore, INDIA

Dr. A. JUSTIN DIRAVIAM
Assistant Professor,
Dept. of Computer Science and Engineering, Sardar Raja College of Engineering,
Alangulam Tirunelveli, TAMIL NADU, INDIA

Editorial Board

Dr. CRAIG E. REESE
Professor, School of Business, St. Thomas University, Miami Gardens

Dr. S. N. TAKALIKAR
Principal, St. Johns Institute of Engineering, PALGHAR (M.S.)

Dr. RAMPRATAP SINGH
Professor, Bangalore Institute of International Management, KARNATAKA

Dr. P. MALYADRI
Principal, Government Degree College, Osmania University, TANDUR

Dr. Y. LOKESWARA CHOUDARY
Asst. Professor Cum, SRM B-School, SRM University, CHENNAI

Prof. Dr. TEKI SURAYYA
Professor, Adikavi Nannaya University, ANDHRA PRADESH, INDIA

Dr. T. DULABABU
Principal, The Oxford College of Business Management, BANGALORE

Dr. A. ARUL LAWRENCE SELVAKUMAR
Professor, Adhiparasakthi Engineering College, MELMARAVATHUR, TN

Dr. S. D. SURYAWANSHI
Lecturer, College of Engineering Pune, SHIVAJINAGAR

Dr. S. KALIYAMOORTHY
Professor & Director, Alagappa Institute of Management, KARAIKUDI

Prof S. R. BADRINARAYAN
Sinhgad Institute for Management & Computer Applications, PUNE

Mr. GURSEL ILIPINAR
ESADE Business School, Department of Marketing, SPAIN

Mr. ZEESHAN AHMED
Software Research Eng, Department of Bioinformatics, GERMANY

Mr. SANJAY ASATI
Dept of ME, M. Patel Institute of Engg. & Tech., GONDIA(M.S.)

Mr. G. Y. KUDALE
N.M.D. College of Management and Research, GONDIA(M.S.)

Editorial Advisory Board

Dr. MANJIT DAS
Assistant Professor, Deptt. of Economics, M.C.College, ASSAM

Dr. ROLI PRADHAN
Maulana Azad National Institute of Technology, BHOPAL

Dr. N. KAVITHA
Assistant Professor, Department of Management, Mekelle University, ETHIOPIA

Prof C. M. MARAN
Assistant Professor (Senior), VIT Business School, TAMIL NADU

Dr. RAJIV KHOSLA
Associate Professor and Head, Chandigarh Business School, MOHALI

Dr. S. K. SINGH
Asst. Professor, R. D. Foundation Group of Institutions, MODINAGAR

Dr. (Mrs.) MANISHA N. PALIWAL
Associate Professor, Sinhgad Institute of Management, PUNE

Dr. (Mrs.) ARCHANA ARJUN GHATULE
Director, SPSPM, SKN Sinhgad Business School, MAHARASHTRA

Dr. NEELAM RANI DHANDA
Associate Professor, Department of Commerce, kuk, HARYANA

Dr. FARAH NAAZ GAURI
Associate Professor, Department of Commerce, Dr. Babasaheb Ambedkar Marathwada University, AURANGABAD

Prof. Dr. BADAR ALAM IQBAL
Associate Professor, Department of Commerce, Aligarh Muslim University, UP

Dr. CH. JAYASANKARAPRASAD
Assistant Professor, Dept. of Business Management, Krishna University, A. P., INDIA

Associate Editors

Dr. SANJAY J. BHAYANI
Associate Professor ,Department of Business Management, RAJKOT (INDIA)

MOID UDDIN AHMAD
Assistant Professor, Jaipuria Institute of Management, NOIDA

Dr. SUNEEL ARORA
Assistant Professor, G D Goenka World Institute, Lancaster University, NEW DELHI

Mr. P. PRABHU
Assistant Professor, Alagappa University, KARAIKUDI

Mr. MANISH KUMAR
Assistant Professor, DBIT, Deptt. Of MBA, DEHRADUN

Mrs. BABITA VERMA
Assistant Professor, Bhilai Institute Of Technology, DURG

Ms. MONIKA BHATNAGAR
Assistant Professor, Technocrat Institute of Technology, BHOPAL

Ms. SUPRIYA RAHEJA
Assistant Professor, CSE Department of ITM University, GURGAON

Title

CONTROLLING THE MENACE OF UNSOLICITED ELECTRONIC MAILS – CONTEMPORARY DEVELOPMENTS AND INDIAN PERSPECTIVES

Author(s)

Sachin Arora
Student,
Rajiv Gandhi School of Intellectual Property law,
IIT Kharagpur, 721302, West Bengal.

Dr. Dipa Dube
Assistant Professor,
Rajiv Gandhi School of Intellectual Property law,
IIT Kharagpur, 721302, West Bengal

ABSTRACT:

The tremendous growth of the Internet as a vehicle of communication in the 1990s to its transformation to a tool with incredible potential has meant that the marketing nuisances of the physical world have also transferred to the digital world in the form of unsolicited commercial electronic messages or simply 'spam'. Majority of spam messages are concerned with commercial advertising and in some ways is analogous to "junk mail" which people receive through the postal system. Unsolicited Commercial Electronic Messages or spam remains undesirable for several reasons. Consumers hate it because it shifts the cost of advertising onto them as they effectively have to pay to download the message. Internet Service Providers dislike spam because it clogs up their systems and slows the traffic down by reducing storage space and bandwidth. Also, spam or unsolicited commercial electronic mail generally contain useless information that one never needs, or market products that one may not require.

The menace of unsolicited commercial electronic mail is relatively new and much before the enactment of spam specific legislations by some countries, liability was imposed only through various tort law concepts, like those of trespass to chattels and nuisance which have been applied by courts in the absence of any statutory regulation. The concept of trademark dilution has also been extended to the act of sending spam using the domain name of some trademarked entity by spammers. Considering the rise of India in the Information Technology sector it is worth mentioning that the need for such a legislative measure to counter this ever growing menace of spam is dire. The industry leaders today who use cutting edge technology to compete with competitors from around the globe cannot afford to waste time on the nuisance posed by unsolicited commercial electronic messages or spam, and therefore we require our laws to take effective measures to neutralize this problem. The present article has delved into the legislative developments in US, EU, Australia and Singapore with regard to spam and emphasized the need for timely action in the Indian sub continent to counter immediate future fallouts.

Key words: Spam, Unsolicited, Liability

INTRODUCTION:

The tremendous growth of the Internet as a vehicle of communication in the 1990s to its transformation to a tool with incredible potential has meant that the marketing nuisances of the physical world have also transferred to the digital world in the form of unsolicited commercial electronic messages or simply 'spam'. The term spam for 'spam mail' was used in the 1990s to describe unsolicited commercial e-mail messages which started to become a problem when the internet was opened up to the general public[1]. Spam or unsolicited commercial electronic messages are those that are frequently sent in bulk; flooding the Internet with copies of the same message and forcing these unwanted messages on Internet users who might otherwise have chosen not to receive them.[2]

Majority of spam messages are concerned with commercial advertising and in some ways analogous to "junk mail" which people receive through the postal system.[3] One of the reasons that spam has become so infamous is that it has often been used for advertising "dubious products, get-rich-quick schemes and other such fraudulent purposes".[4] Spammers target both groups, by mass mailing the spam simultaneously to multiple groups and individual users with direct mail messages.

Consumers hate unsolicited mail (Spam) because it shifts the cost of advertising onto them as they effectively have to pay to download the message. Internet Service Providers hate it because it clogs up their systems and slows the traffic down by reducing storage space and bandwidth. For instance in a US case,.[5] an email that would normally have been delivered in minutes took three days. Such reduced performance creates irate customers who may move to another provider in what is a highly competitive market.

As per one of the reports by the European Union's Internal Market Commission, the costs to internet users worldwide because of 'spam' amounts roughly upto €10 billion per

[1] Jan H. Samoriski, *Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?*, 43 J. Broadcasting & Electronic Media 670 (1999)
[2] Karnika Seth, *Spam - Need for an Effective Legislation ,at* http://www.sethassociates.com/spam-need-for-an-effective-legislation.html (last visited Mar. 26, 2010)
[3] *See supra* note 1 ("Junk e-mail is often analogized to the junk mail delivered by the U.S. Postal Service").
[4] *See supra* note 2
[5] *Compuserve Inc*. **v.** *Cyber Promotions Inc.* 962 F. Supp. 1015 (S.D. Ohio 1997).

year.[6]Another report of a 2004 survey pointed out that the cost of spam to United States alone is $21.58 billion annually, while another estimated the cost at $17 billion, up from $11 billion in 2003[7]. In 2004, the worldwide productivity cost of spam has been estimated to be $50 billion in 2005.[8]An estimate of the percentage cost borne by the sender of marketing junk mail is 88%, whereas in 2001 one spam was estimated to cost $0.10 for the receiver and $0.00001 (0.01% of the cost) for the sender.[9]Thus it is not surprising that many of the developed countries of the world with high penetration of internet have enacted laws to regulate the menace of unsolicited mails over the internet. Courts also have evolved their own theories for countering this over growing menace by deciding that spam e-mail can constitute a trespass of the service provider's personal property, because of the degradation in the systems performance.

The present paper has attempted a comparative analysis of the legislative and judicial measures of the countries including United States of America, European Union, Australia and Singapore, along with a scrupulous glance at the Indian legal scenario. The study is of particular interest in present times because of the void created since the onset of the digital revolution in India with regard to unsolicited commercial electronic mails and the potential dangers posed in the circumstances. The Information Technology Act, 2000 has failed to address the problem of unsolicited mails and the existing laws are unsuited to the needs of the times. Do we require a new law to combat the menace, in line with the other nations, is a big question which the present study has attempted to address.

SPAM:

SPAM is a term used to refer to the abuse of the electronic message delivery systems by sending unsolicited messages in bulk, indiscriminately. While this term may mostly be used in the context of e-mail only, but spam includes other forms of unsolicited messages as well,

[6]*See , Data protection: "Junk" e-mail costs internet users 10 billion a year worldwide - Commission study , available at* http://europa.eu/rap*Id*/pressReleasesAction.do?reference=IP/01/154&format=HTML&aged=0&language=EN&guiLanguage=en, (last visited Mar. 24, 2010).

[7]*See* Thomas Claburn, *Spam costs billions, available at* http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?article*ID*=59300834 (last visited Mar. 24, 2010)

[8]*Id*

[9]*See* Rebecca Lieb, *Make spammers pay before you do, available at* http://www.clickz.com/1432751 (last visited Mar. 24, 2010)

including instant messaging spam, spam in blogs, file sharing network spam, mobile phone messaging spam, Internet forum spam and social networking spam.[10] The e-mail spam which is also known as 'junk mail' or 'unsolicited commercial e-mail (UCE)' is the practice of sending frequent unwanted e-mail messages with commercial content to a large number of recipients. With the invention of the Internet and e-mail, advertisers were provided with a very cost effective means of reaching potential customers no-matter where they might be located on the globe. All that is required to send such unsolicited commercial messages is an internet connection and a list of e-mail addresses. As a result of the low start-up cost and ease of obtaining worldwide access, internet mass marketing companies send billions of unsolicited commercial e-mail messages much to the dismay of Internet Service Providers and e-mail subscribers alike[11]. When spam reaches an Internet Service Provider (ISP) for delivery to a subscriber, the subscriber must access, review, and either save, return, or discard the unsolicited mail. Until the subscriber processes the unsolicited message, the spam occupies part of the limited amount of storage space on an ISP's computer network. Once the subscriber has reviewed the spam, he may wish to return it to its sender. However, because spammers often use false return e-mail addresses,[12] the returned spam bounce back to the ISP's server as undeliverable mail, which once again depletes the ISP's limited storage capacity. The sending of large amounts of spam, or "bulk spam," can so reduce the availability of resources available to the ISP leading the network to crash or operate at a significantly diminished capacity.[13] Such reduced storage capacity can result in a decrease in the quality of the Internet service provided; thereby creating unsatisfied customers who may choose not to renew their subscriptions.

The deluge of spam places a heavy burden on ISPs who must reroute or delete each piece of unclaimed or rejected junk e-mail that reside on their server. Moreover, since many e-mail subscribers pay for Internet access on a per minute or per hour basis, using those paid minutes to access, review, and return or discard unsolicited mail that was deposited into their e-mail accounts is, in essence, paying for spam[14]. Consequently, subscribers rightfully become annoyed

[10] *See Report on Spam Sending Countries*, *available at*http://blog.alertsec.com/2010/03/report-on-spam-sending-countries/, (last visited Mar. 26, 2010)
[11] *America Online, Inc*. **v**. *IMS*, 24 F. Supp. 548, 549
[12] *People* **v**. *Lipsitz*, 663 N.Y.S.2d 468, 471
[13] *Cy ber Promotions, Inc.***v**. *America Online, Inc.*, 948 F. Supp. 436, 438.
[14] Jeffery L. Kosiba, *Legal Relief from Spam Induces Internet Digestion*, 25 Dayton L. Rev. 187(1999).

by the volume of spam they receive and attempt to rectify the problem by entreating the ISP or the spammer to cease and desist.[15]

COMBATING THE MENACE OF SPAM –A COMPARATIVE OVERVIEW:

The US Scenario Unsolicited e-mail is regulated at both the federal as well as the state levels. More than half the states have their own laws dealing with the menace of such unsolicited mails including the likes of Washington, Delaware, Virginia and Wiscosin[16]. The law governing unsolicited e-mail at the federal level is the CAN-SPAM Act. Owing to both public pressure as well as the industry to regulate unsolicited electronic mails, the Congress passed the CAN SPAM Act in December 2003[17]. Though before the onset of this Act many technical solutions had also been tried to counter the ever-growing menace of spam and put a stop to it, but to no avail. While proving to be quiet effective these measures were still found to be inadequate.[18] One of the leading service providers MSN.com claimed that the top most complaint made by its subscribers was spam.[19] They also feared that a substantial number of its subscribers were willing to shift to alternative e-mail service providers if they provided better anti-spam facilities, thus compelling the ISP to direct its resources and machinery towards eliminating spam as its reputation was at stake.

The efforts of various ISPs in removing spam received a further boost with the decision of *Cyber Promotions* v. *AOL*[20]which denied the 'right to spam'. The decision gave the ISPs legal authority to use spam filtering and blocking policies using any resources which were treated by the court as private and not public. They also started vigilance on their part sending notices to

[15] *Id*
[16] See Cal. Bus. & Prof. Code § 17529 (West 2003); 815 Ill. Comp. Stat. 511 (2000); Wash. Rev. Code § 19.190.060 (2003); Va. Code Ann. § 18.2-152.3:1 (Michie 2003); Wis. Stat. § 944.25 (2001); Del. Code Ann. tit. 11, § 937 (2003)
[17] Controlling the Assault of Non-Solicited Act of and Marketing Pornography (CAN-SPAM) 2003 Act §§ 2-14, 15 U.S.C.A. §§ 7701-7713 (Supp. VI 2004).
[18] Rebecca Bolin, *Opting out of Spam: A Domain Level Do-Not-Spam Registry*, 24(2) YALE LAW & POLICY REVIEW 399 (2006).
[19] Brandon Sprague, *Microsoft Attacks Spam in Courts*, SEATTLE TIMES. Aug. 2. 2004, *available at* http://seattletimes.nwsource.com/html/businesstechnology/2001994497_microspam02.html
[20] 948 F. Supp. 436 (E.D. Pa. 1995)

mass junk mailers or by shutting them down.[21] Access of subscribers to suspected website of spammers was also blocked by some ISPs.[22] Some ISPs, on the other hand, reserved with them the right via contracts to remove any content without notice to the user.[23] Expensive spam filters were also developed by some ISPs to identify and delete spam on the go e.g., use of patented technology of Microsoft 'SmartScreen' for its incorporation in its e-mail service called Hotmail to the use of the open source called 'SpamAssasin' by others[24].

Even though the earlier mentioned steps taken by ISPs to combat spam were effective, yet they left a want for an effective federal legislation. The numbers of spam mail, just kept on surmounting stupendously. In September 2001, spam was only 8% of the total emails being sent while by December 2003, this number rose to much higher levels.[25]Hotmail alone put on an estimate to delete 95% of all incoming email.[26] These spam filters provided and still do provide businesses with the much needed impetus to enhance productivity by not wasting away their resources in sorting and filtering out unwanted email. The spam filtering process was further aided by freely available blacklists which contain a pre-compiled list by its makers of a number of servers known to send spam mail and which in their opinion should be blocked by the ISPs.[27] The counterpart of the blacklist was the whitelist containing a list of approved senders and mandating the ISP to make sure that the mails of such senders do not get caught in the anti-spam

[21] Jan Samoriski, *Issues in Cyberspace: Communication, Technology, Law and Society on the Internet Frontier*, (Boston: Allyn and Bacon, 2002).

[22]Jonathan Krim, *AOL Blocking Links as Anti-Spam Tactic* MIAMI HERALD, March 21 2004, *available at* http://nl.newsbank.com/cgi-bin/ngate/MH?ext_docid=%3Ca%20href=%27/nojavascript.html%27%20onclick=%27ngate(%271018023D64B75A77%27,%27AOL+BLOCKING+LINKS+AS+ANTI-SPAM+TACTIC%27,%271%27,%27The+Miami+Herald%27,%27MH%27,%27MH%27,%27%27,%27%27,%27MH%27);%20return%20false;%27%3E&ext_hed=AOL%20BLOCKING%20LINKS%20AS%20ANTI-SPAM%20TACTIC&s_site=miamii&ext_theme=realcities2&pubcode=MH.

[23]*See*, e.g., Yahoo! Terms of Service § 6, http://docs.yahoo.com/info/terms/ (last visited Mar.24, 2010) ("You acknowledge that Yahoo! may or may not pre-screen Content, but that Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or move any Content that is available via the Service.").

[24] Paul Thurrott, *What You Need to Know About Microsoft SmartScreen Technology and the Exchange Intelligent Message Filter ,at* http://www.windowsitpro.com/article/exchange-server/what-you-need-to-know-about-microsoft-smartscreen-technology-and-the-exchange-intelligent-message-filter.aspx, (last visited Mar. 26, 2010)

[25] Bill Gates, *Presenting and Enhancing the benefits of e-mail A Progress Report* (Jun. 28, 2004), *available at*http://www.microsoft.com/mscorp/execmail/2004/06-28antispam.mspx, (last visited Mar. 26, 2010)

[26]*Id*

[27]*See Yale Univ. Support Servs., Spam Management: RBL Rejection Process*, *available at*http://www.yale.edu/email/spam/rblprocess.html (last visited Mar. 26, 2010)

filters.[28]Another alternative proposed was e-mail postage which is a recent idea being implemented by the likes of Yahoo and AOL where the sender of e-mail needs to pay a certain amount of fee just like a postage stamp over each e-mail sent.[29]

Apart from the technological measures adopted to combat spam, ISPs also brought several civil and criminal suits before the enactment of the federal CAN-SPAM Act to impose liability on senders of spam. The suits involved multiplicity of legal concepts from both common law, including tort of trespass and nuisance, as well as statutes i.e., trademark dilution under the Lanham Act.

One such landmark case was *Compuserve* v. *CyberPromotions*[30]. In this case, even after repeated requests the defendant continued to send large volumes of mails circumventing Compuserve's technical blocking measures. The court while granting injunction in favour of the plaintiff held that the sending of emails amounted to illegal trespass of the plaintiff's property and caused sufficient damage to its servers. The doctrine was to be followed in what was to be a series of victories subsequently relying on the verdict of this case[31]

Intel Corp v *Hamidi*[32] on the other hand crushed the doctrine of trespass of chattels applied to spam email. In this case, Kourosh Hamidi, who happened to be an ex-employee of Intel, sent six e-mails to a set of 35000 Intel employees denouncing Intel. However, the impact of his act was found to be negligible on the Intel Servers. The court ruled that the damage to the servers and Intel's interests in its network were insufficient to support a trespass to chattels claim. This meant that only the most aggressive spammers causing actual damage to networks were committing trespass to chattels.

[28] Thomas Claburn,*Microsoft Signs on for E-Mail Program: Hotmail and MSN Added to List of Distributors that Send Legitimate E-Mail Messages*, INFORMATIONWEEK, May 10, 2004 at 30,*available at* http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?article*ID*=20000255 (last visited Mar. 26, 2010)

[29] Mike Musgrove, *Paid E-Mail Seen as Sign of Culture Change; Guaranteed Delivery Plans by AOL, Yahoo Viewed as Part of End to Openness*, WASHINGTON POST. Feb. 7, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601539.html

[30]*CompuServe, Inc.***v**. *Cyber Promotions*, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

[31]*AOL, Inc*. **v.** *LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998) (awarding summary judgment for trespass to chattels, Lanham Act claims, and other claims); *America Online, Inc.* **v.** *Prime Data Systems, Inc*., 1998 WL 34016692 (E.D. Va. 1998) (awarding injunctive relief for trespass to chattels)

[32]71 P.3d 296 (Cal. 2003).

In another case[33], AOL was successfully able to bring about action against a spammer on the theories of trademark law, such as trademark dilution and false designation of origin. AOL alleged that the defendant improperly sent over 60 million unauthorized e-mail messages to AOL subscribers. The court held that defendant's use of the AOL domain name trademark in their message headers created a "false designation of origin" in violation of trademark law because any subscriber seeing the familiar domain name in the header would mistakenly conclude that the spam either originated with or was sponsored by AOL. The court also determined that AOL used its famous trademark as a domain name and concluded that because AOL's customers made negative associations between their ISP and the junk e-mail sent by IMS, defendant's use of the domain name tarnished the mark resulting in the dilution of its distinctiveness.

In certain other cases, the Federal Trade Commission pursued cases of spam on charges of fraud. By the end of 2004, the FTC had brought about a total of 35 cases against spam mailers on account of fraud[34]. Earthlink, another e-mail service provider, also successfully brought about two different actions against spammers winning 25 million and 16 million dollars in Kentucky and New York judgment respectively.[35]However, Earthlink was not able to execute both the judgments even after the passing of two years. The results of Microsoft's legal efforts were similar. It won six default judgments, one summary judgment, and settled four claims, while one case was dismissed.[36] The summary judgment was for $4 million against Daniel Khoshnood who sent millions of emails claiming to be Microsoft. Microsoft did collect some $500,000 in settlements,[37] but while it won around $54 million in damages, it collected very little of that figure. To this day, Daniel Khoshnood remains on the list of the top 200 spammers.[38]

The CAN-SPAM Act of 2003 being a federal law has nationwide coverage. The Act was passed on account of problems with interstate jurisdiction on spam governance, as e-mail

[33]*America Online, Inc.* **v.** *IMS* 24 F.Supp.2d 548.
[34]Spam (Unsolicited Commercial E mail)*:* Hearing Before the S. Comm. on Commerce, Science, and Transportation, 108th Cong., May 21, 2003 (testimony of Mozelle W. Thompson, Comm'r, Federal Trade Commission), http://commerce.senate.gov/hearings/testimony.cfm?*Id*=773 &wit_*Id*=2089.}
[35] Ryan Mahoney, *EarthLink Sues Alabama Spammers*, BIRMINGHAM J. (Ala.), Sept. 5 2003 at 5.
[36]Matt Hines, *Microsoft Awarded $4 Million in Spam Suit*, NEWS.COM, *available at* http://news.com.conVMicrosofHawarded+4+million+in+spam+suit/2 10 14_3-5272776.html, (last visited Mar. 26, 2010)
[37] Cathleen Flahardy, *Software Giant Leads the Pack in Spam Eradication: Microsoft Teams With Amazon to fight Spammers in court.*, CORP. LEGAL TIMES, Dec. 2004, at 20.
[38]*See,* The Spamhaus Project, ROKSO List, http://www.spamhaus.org/rokso/index, (last visited Mar. 26, 2010).

addresses have no geographic boundaries in cyberspace which would have serious implications for Internet governance both nationally and internationally.[39]

The Preamble to the Act clearly sets out its objectives:

"*To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.*"

The statute basically aims at regulating e-mails, the primary purpose of which is commercial advertisement or promotion of a commercial product or service.[40] There are no quantitative restrictions and the Act applies whenever an advertiser sends any e-mail message.[41] The Act bans some deceptive practices, chiefly being prohibition of forged headers[42] and deceptive subject lines.[43] It does not generally prohibit false or deceptive messages, although such messages would likely be subject to state deceptive trade practices laws or the Lanham Act prohibition of unfair competition[44]. The CAN-SPAM Act also lets states enact laws specific to email that prohibit falsity or deception in commercial messages.[45] The Act also extensively regulates the structure of spam messages and the techniques used to send them. It requires spam to contain a method for recipients to opt out of later messages and to contain identifying information, including the sender's physical mailing address[46]. It also prohibits methods used to build email lists and evade detection, including harvesting addresses from web pages and Usenet newsgroups, and using so-called dictionary attacks to send spam to thousands of e-mail addresses[47], automatically creating multiple e-mail accounts for the purpose of sending spam messages,[48] and transmitting messages through third party computers without authorization.[49] The Act also empowers the Federal Trade Commission (FTC) being the regulatory agency with wide-ranging powers to create and enforce a wide variety of rules under various consumer

[39]Taiwo A. Oriola, *Regulating Unsolicited Commercial E-mail in United States and the European Union: Challenges and Prospects*, 7Tul. J. Tech. & Intell. Prop. 113, 2005
[40]CAN SPAM Act, § 3(2)(a).
[41] *Id* §4(a)(1.
[42] *Id* §5(a)(1).
[43]*Id* §5(a)(2).
[44] 15 USC § 1125 (2000)
[45]*See supra* note 40, § 8
[46]*Id* §5(a)(3)(A).
[47]*Id* §5(b)(1).
[48]*Id* §5(b)(2).
[49]*Id* §5(b)(3).

protection legislations. The FTC is also authorized to establish a "do-not-email" registry, but not compulsorily required to make such a registry.[50]

The Act permits for civil enforcement by both federal and state agencies[51] as well as criminal provisions. Private Citizens and businesses on the other hand receiving spam do not have the power of enforcement. The penalties for conviction for any of these offenses is a fine or imprisonment for not more than 5 years or both, if the offense is committed in pursuance of any felony under the laws of the United States or of any state, or the defendant has had previous convictions for sending multiple commercial e-mail messages, or unauthorized access to any computer system.[52]. The Act is quiet comprehensive and includes nearly every type of antispam measure possible; though it falls short on one such instance and that being an outright ban on spam and permits the sending of legitimate spam.

The Act also allows for enforcement provision for ISPs. It provides for statutory damages for upto $100 per false or misleading message received and upto one million in total.[53] The plaintiff is also entitled to seek treble damages if the defendant 'knowingly' and 'willfully' violated the law.[54] Courts have also been granted the discretionary power to grant attorney fees under the Act.[55]

One of the most important provisions of this Act is the pre-emption provision enshrined in Section 8 (b)(1). It reads as follows:

"*This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent or that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.*"[56]

The provision has two parts. The portion up to "except" defines the outer boundary of preempted state laws: any state law "that expressly regulates the use of electronic mail to send

[50] *Id* § 9.
[51] *Id* § 7(a)-(d).
[52] *Id* §4(a).
[53] *Id* §7(g)(3)(A)-(B).
[54] *Id* §7(g)(3)(C).
[55] *Id* §7(g)(4).
[56] *Id*§ 8(b)(1).

commercial messages" is at least potentially preempted, while any that does not, is not.[57] The latter portion of the provision, the savings clause, protects state laws that otherwise would be preempted if they fall into certain categories.

The hard question in determining the scope of the entire provision is the scope of its savings clause. Section 8(b)(1) expressly preserves state laws that prohibit" falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[58] This clause could be interpreted in multiple ways, and how it is interpreted will have a substantial effect on states' ability to target spam. The section's effect on state law enforcement methods is also unclear.

The provision clearly preempts a substantial portion of state spam laws. For instance, the broadest provision of California's law, which went into effect January1, 2004, and would have banned sending any commercial email advertisement without the recipient's direct statute expressly regulates consent, is clearly preempted. California's the use of electronic mail, and it goes far beyond prohibiting falsity or deception. At the same time, many more narrowly drawn state laws survive, and it is these provisions that must be effective against spam.

The enactment of this federal law has also raised a few issues. Section 5(a)(1) of the CAN-SPAM Act prohibits the transmission of unsolicited commercial electronic messages whose header information is materially false or materially misleading. Furthermore, the Act in section 3(8) defines “header information” as “the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.” Thus in effect the above provision would invariably result in revealing the online identity of the sender of spam mail. This has endangered the anonymity of persons communicating over the internet which has been recognized by the US courts as freedom of speech being a constitutional right enshrined in the first amendment.[59] However the maintenance of anonymity would also pose some challenges in cyberspace as there might be a tendency towards it misuse. With no danger of disclosing the source of mail which may be used as such to identify the sender mail with false descriptive

[57]Roger Allen Ford, *Preemption of State Spam Laws by Federal CAN-SPAM Act*, 72 U.CHI..L.REV.355(2005)
[58]*Ibid.*
[59]*McIntyre* **v.** *Ohio Elections Commission*, 514 U.S. 334 (1995).

headers may be sent enticing the recipient to open up sexually oriented content in the name of insurance policy or house hold items.[60] It is not disputed that the primary aim of section 5(a)(1) of the CAN-SPAM Act is the prohibition of fraudulently misleading header information in unsolicited commercial e-mails which is in public interest. However the provision is narrowly defined as it affects only the commercial unsolicited e-mails. Thus non commercial e-mails would be free from its ambit and thus considered as part of free speech.

Another issue is that the CAN-SPAM Act does not completely override the state spam laws. It will operate concurrently and will not preempt state spam laws that prohibit false and deceptive commercial e-mail messages. However it will put upto to question as to the power of state attorneys to prosecute a case if it is taken up by the FTC. It is therefore inevitable that issues would be raised about the propriety of state spam laws in the context of the Commerce Clause of the United States Constitution. Article 1, Section 8, Clause 3 of the Constitution empowers Congress "to regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."[61] The Commerce Clause essentially provides the basis that prohibits states from regulating in ways that hamper interstate commerce, even in the absence of Congressional action.

In the Ferguson case[62], the plaintiff, an e-mail recipient, sued the defendants for sending him deceptive and misleading unsolicited e-mails in contravention of California law. The defendants challenged the lawsuit, on grounds that the statute in question violated the dormant Commerce Clause of the United States Constitution. The court found that section 17538.4 of the California Business and Professions Code did not discriminate against or directly regulate or control interstate commerce. In fact the Californian law was not a burden but facilitated interstate commerce which was in public interest and thus did not violate the dormant commerce clause. The court held that the California statute "does not regulate the Internet or Internet use per se. It regulates individuals and entities who (1) do business in California, (2) utilize equipment located in California and (3) send UCE to California residents and thus any extra-territorial reach of such law is justified. The CAN-SPAM Act's preeminence over state spam laws can effectively foreclose possible clashes between the disparate states spam laws and

[60] *FTC* **v.** *Westby*, No. 03 C 2540, 2004 WL 1175047 (N.D. Ill. May 6, 2004)
[61] U.S. Const. Art. 1, § 8, cl. 3.
[62] 115 Cal. Rptr. 2d 258 (Ct. App. 2002).

the Commerce Clause. The Act transcends the constitutional impasse posed by the Commerce Clause to state spam laws. Its homogeneity vis-à-vis state spam laws offer a comparatively better front in the fight against spam.[63]

On summarizing the above given it would be fair to say that even though several state legislations dealing with the menace of spam were already present yet the United States chose to enact a federal legislation. The CAN-SPAM does not completely override existing legislations but only pre-empts them to a certain extent. The Act requires the commercial messages to be labeled and to contain opt out messages for the recipient. The Act also prohibits the use of deceptive subjective lines and false header messages.The Act also empowers the Federal Trade Commission (FTC) being the regulatory agency with wide-ranging powers to create and enforce a wide variety of rules under various consumer protection legislations. The FTC is also authorized to establish a "do-not-email" registry, but not compulsorily required to make such a registry.

Spam in EU:

Spam is regulated by the Electronic Personal Data and Privacy Directive 2002/58/EC (E-Privacy Directive) in the European Union. [64] The directive covers all public electronic communications, and not just the Internet and computers. However, antispam provisions that are similar to the key provisions in the E-Privacy Directive can be found scattered in previous directives generally regulating electronic commerce.[65]

One of the primary provisions of the E-Privacy Directive is the requirement of prior consent of subscribers before transmission of unsolicited commercial e-mails for direct marketing. This is commonly known as ‘opt in’ consent-based e-mail traffic control, as opposed to ‘opt out’ nonconsensual approach adopted by the CAN-SPAM Act. One of the reasons for the

[63] *Id*

[64] Council Directive 2002/58/EC, on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37

[65] *See* Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, art. 6, 2000 O.J. (L 178) 1. Article 6(a) of this directive requires that “commercial communications” be clearly *Id*entified as such. See also Council Directive 84/450, 1984 O.J. (L 250) 17 (concerning misleading advertising); Council Directive 95/46 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31; Council Directive 97/7 on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19.

adoption of such a 'opt in' policy which also happens to be the policy of the European electronic commerce governance was protecting the privacy of Internet users. However, whether or not the opt-in policy would survive the European Court of Justice (ECJ) would invariably depend on whether or not the Court perceives it as a restriction on advertising rules. In *Konsumentombudsmannen* (*KO)*v. *Gourmet International ProductsAB,*[66] the European Court of Justice (ECJ) held that a prohibition of all advertising directed at consumers (such as advertisements in the press, on the radio, and on television, the direct mailing of unsolicited material, or the placing of posters on the public highway) of alcoholic beverages, the consumption of which is linked to traditional social practices and to local habits and customs, is liable to impede access to the market by products from other member states more than it impedes access by domestic products, with which consumers are instantly more familiar. The Court further held, however, that such a restriction could be justified on grounds of public health protection.[67]

The second provision for the E-privacy directive allows businesses to use customers' electronic contact details which have been acquired during the course of commercial transactions for future direct marketing of similar products or services. However, customers must be given an opportunity to object free of charge to such use of their electronic contact details.[68] Since the prior consent of the customers is essential for its implementation it is very much in line with the 'opt in' policy. Thus the directive seeks to maintain a balance between the customer's privacy rights and legitimate advertising by businesses.

The third provision of the directive deals with the prohibition of disguising or concealment of the identity of the sender of unsolicited e-mail messages, or the sending of an unsolicited electronic mail without a valid return address of the sender's e-mail for the purpose of direct marketing. This is something similar to Sec 5 of CAN-SPAM Act and may raise similar issues of anonymity and free speech in Europe.

Article 15(2) of the E-Privacy Directive incorporates article 22 of the Data Protection Directive, which allows individuals in member countries to sue for an alleged breach of any of the provisions of national antispam legislations. This is a marked difference from the CAN-

[66]C-405/98 [2001] 2 CMLR 31
[67]Case C-405/98, 2001 E.C.R. I-1795 (2001).
[68]*See supra* note 65, Article 13(2).

SPAM Act, where there is no express statutory right to file a civil suit for an alleged infringement of any of its provisions.

The E-Privacy directive of the European Union requires the member states to follow three key provisions. The first being the pursuance of an 'opt in' policy as opposed to the US 'opt out' policy which requires the prior consent of the subscribers before sending them unsolicited e-mail. The second provision allows businesses to use contact details to send e-mails for future transactions provided the customers have no objection to it. The third provision prohibits the sending of unsolicited e-mail without proper headers or such other information which results in concealing of the identity of the sender.

Spam in Australia:

In 2003, the Government of Australia brought about an antispam legislation in response to certain community concerns about the growing menace of spam or unsolicited commercial electronic message and its impact on the effectiveness of electronic communication and the costs imposed on end users.[69] The Spam Act 2003[70] lays down the guidelines for sending legitimate commercial electronic messages and prohibits the sending of unsolicited commercial electronic messages whether they are in the form of mobile phone messages including both text and multimedia messages and e-mail; however normal voice to voice messages over phone are outside the ambit of the Act. Even a single unsolicited commercial electronic message is considered to be spam and the requirements under the Spam Act apply to all commercial electronic messages, including both bulk and individual messages.

The Australian Act defines a commercial electronic messages as those messages that offer to supply goods or services, or which advertise goods and services, land or business or investment opportunities, or which direct the recipient to a location where goods and services are

[69] *See Department of Communications Spam Act 2003 Review Issues Paper,available at*http://www.dbcde.gov.au/__data/assets/pdf_file/0020/34418/Spam_Review_Issues_Paper.pdf (last visited Mar. 26, 2010)

[70] Spam Act 2003, Act No. 129 of 2003 (Cth.)

sold or advertised, or which are to assist or enable a person to dishonestly obtain property, financial advantage or a gain from another person.[71]

The Act applies to only those messages which have an 'Australian link' present. This includes both messages that originate or are commissioned in Australia being sent to any destination; and messages that originate or are commissioned overseas being sent to an address accessed in Australia.[72]

There are three main requirements laid down under the Act for sending commercial electronic messages. The first such requirement being that such messages be sent with the consent of the addressee.[73] Consent may be expressly given by the recipient, or under certain restricted circumstances it may be inferred from the conduct or business relationships of the recipient.[74] The second requirement is that all messages with an 'Australian link' present must be containing information which can identify the sender of the message and that such information be likely to remain correct uptil 30 days after the sending of the message.[75] The third requirement is that an unsubscribe facility or 'opt out; mechanism be provided in such messages allowing people to opt out from receiving messages from that source in the future which is in lines with the CAN-SPAM Act.[76] The Act requires that a request to unsubscribe must be honored within five working days. The unsubscribe facility must be reasonably likely to be able to receive and act on unsubscribe messages for a period of 30 days after the sending of the message.

In addition to the above mentioned requirements the Spam Act 2003 also prohibits the sending of a commercial electronic message to a non-existent address that would have an Australian link if the address existed. It is also prohibited to aid, abet or otherwise be party to a contravention of the legislation.[77] The Act also prohibits the use, supply or acquisition of harvesting software which have been described in the analysis of Singapore legislation.

The Spam Act also makes exceptions in case of some messages which have been given the label of 'designated commercial electronic messages' and are sent by either government

[71] *Id* §6
[72] *Id*, §7
[73] *Id*, §16
[74] *Id* Schedule 2.
[75] *Id* §17
[76] *Id* §18
[77] *Id*

bodies, registered political parties, charities, religious organizations or educational institutions in certain circumstances. Such designated electronic messages are not are not required to have the addressee's consent, but they must still carry accurate information to identify the organization or individual that authorized the sending of the message. However to be considered a 'designated electronic message' it is necessary for the message to be in respect of goods or services that are being supplied by one of the organizations listed above[78].

The Australian Communications and Media Authority (ACMA) is the statutory authority responsible for enforcing the Act.[79] The ACMA also has a legislative role in facilitating and supporting the development of industry codes that complement the Act. Such industry codes provide relevant and achievable standards and procedures to assist compliance with the legislation, as well as procedures for the handling of complaints.

The Spam Act also includes provisions that provide for Australia's participation in multilateral arrangements with other countries concerned with the regulation of spam, pursuant to which Australia has entered into many international agreements aimed at regulating the menace of unsolicited commercial electronic mail[80] e.g., UK, US and Australia-tripartite MoU on spam in July 2004, Australia and Thailand-joint statement on telecommunications and information, The London Action Plan on Spam- October 2004 and Seoul-Melbourne Multilateral MoU for Asia Pacific region in April 2005.

One of the significant cases under the Spam Act 2003 creating significant case laws under the Australian spam statute was *Australian Communications and Media Authority* v. *Clarity1 Pty Ltd*[81]. The case basically involved the retrospective application of provisions under the Act relating to the acquisition and use of harvested address lists. It was held by Justice Robert Nicholson AO that lists gathered or acquired prior to the Act coming into force are still subject to the legislation. It also clearly struck down the respondents defense that he had obtained consent to use the gathered addresses for the defined purpose, and also noted a lack of compliance with the provisions of the act requiring the provision of a functional unsubscribe facility.

[78] *Id* Schedule 1
[79] *Id* § 42
[80] *Id* § 45.
[81] [2006] FCA 410.

The Spam Act 2003 provides guidelines for sending legitimate commercial electronic messages and prohibits the sending of unsolicited commercial electronic messages, whether by email, instant messaging, short message service (SMS), or multimedia messaging. Under the Act, messages must be sent with consent and even a single unsolicited commercial electronic message is considered to be spam. The Act empowers the Australian Communications and Media Authority (ACMA) for enforcing the Act. The Act also lays down a peculiar requirement for messages with an "Australian link" to contain such information so as to identify the sender apart from pursuing the usual 'opt out' policy.

Spam in Singapore:

A survey was conducted by the Info-communications Development Authority (IDA) to determine the spread of spam in Singapore.[82] It was brought to light that spam had cost the Singapore economy close to $23 million dollars affecting close to 94% of e-mail users in Singapore.[83] These statistics led the legislators of this small nation to enact the Spam Control Act 2007.[84] Substantial portions of this Act are either based on the Australian Spam Act[85] or the US CAN-SPAM Act. The Act in line with the federal US legislation seeks to regulate and not prohibit unsolicited communication. Also, as opposed to the opt-in policy being pursued by the European Union in the EC Directives, the legislators favored the opt-out approach as it was much more suitable to the business environments of Singapore.[86] The Act is concerned with unsolicited electronic messages which include both messages sent to a mobile phone or e-mail sent to an e-mail address.[87] Whether the unsolicited electronic message is commercial or not is to be judged having regard to the content of the message, the reference content (by way of links provided in the message, to websites and other sources) and the way in which the message is presented.[88] The message will be considered as commercial if the primary purpose is to offer to

[82] *See Info-communications Development Authority of Singapore, "2003 Survey on Unsolicited E-mails" (25 May 2004), online: IDA Singapore, available at* http://www.ida.gov.sg/Policies%20and%20Regulation/20061006143023.aspx (last visited Mar. 26, 2010)
[83] *Id*
[84] Spam Control Act 2007, No. 21 of 2007
[85] Act No. 129 of 2003 (Cth.).
[86] Karthik Ashwin Thiagarajan, *Spam Control Act 2007*, 2007 Sing. J. Legal Stud. 361 (2007).
[87] *See supra* note 70, § 4(1) read with § 2.
[88] *Id*. § 3(1).

provide or supply, or to advertise or promote certain types of subject-matter including goods, services, land, interest in land, business or investment opportunity, or advertising the provider or supplier (existing or prospective) of any such subject-matter.[89] The Act also labels any electronic message the primary purpose of which is to assist or enable, "a person, by deception, to dishonestly obtain property belonging to another person"[90] or to "dishonestly obtain a gain from another person"[91] to be commercial. However certain numerical thresholds have to be reached before an unsolicited commercial message can be considered to be sent in bulk.[92] These thresholds have been provided in section 6 which defines "sending in bulk" to mean, sending of (a) more than 100 electronic messages containing the same or similar subject-matter during a 24-hour period; (b) more than 1,000 electronic messages containing the same or similar subject-matter during a 30-day period; or (c) more than 10,000 electronic messages containing the same or similar subject-matter during a one-year period..[93]

Section 11 of the Act requires the senders of bulk unsolicited commercial electronic messages to comply with the requirements laid down in the second schedule of the Act[94]. Such requirements chiefly being that the message being sent should contain e-mail address, Internet location address, telephone number, facsimile number or postal address that a recipient may use to submit an "unsubscribe request" in order to stop receiving any further unsolicited commercial electronic messages from the sender. The existence of the unsubscribe facility has to be brought to the specific notice of the recipient in a "clear and conspicuous manner," through a statement in the English language and any other language that is used in the message.[95] The sender is prohibited from sending any further such messages to the concerned recipient ten days after the day on which the unsubscribe request is submitted[96] and is not allowed to provide any third party with any information in the unsubscribe request. The Act also requires that all unsolicited

[89] *Id*
[90] *Id* § 3(1)(x).
[91] *Id* § 3(1)(xii).
[92] *See supra* note 70, § 6.
[93] *Id*
[94] *See supra* note 70 Second Schedule, para. 2
[95] *Id*
[96] *See supra* note 70 Second Schedule, para. 2(7).

commercial electronic messages need to indicate at the very outset that they are commercial in nature through a fixed format label.[97]

The Act further totally prohibits sending of any electronic message through dictionary attack or address harvesting software. [98] A dictionary attack refers to generation of e-mail addresses or mobile phone numbers by using permutations and combinations of letters, number and other characters.[99] Address harvesting software on the other hand are softwares that trawl and collect electronic addresses from the Internet.[100]

As far as the territorial applicability of the Act is concerned, it applies only to those electronic messages that have a "Singapore link" present.[101]It attempts to prohibit the abuse of communication infrastructure within Singapore as well as have extraterritorial effect by bringing such individuals and entities under the ambit of the Act which qualifies the requirement of possessing a "Singapore Link".[102] The message is to contain a Singapore link if [103]

(a) the message originates in Singapore;

(b) The sender of the message is (i) an individual who is physically present in Singapore when the message is sent; or (ii) an entity whose central management and control is in Singapore when the message is sent;

(c) The computer, mobile telephone, server or device that is used to access the message is located in Singapore;

(d) The recipient of the message is (i) an individual who is physically present in Singapore when the message is accessed; or (ii) an entity that carries on business or activities in Singapore when the message is accessed; or

(e) If the message cannot be delivered because the relevant electronic address has ceased to exist (assuming that the electronic address existed), it is reasonably likely that the message would have been accessed using a computer, mobile telephone, server or device located in Singapore.

[97] *See supra* note 70 Second Schedule, para. 3(1).
[98] *See supra* note 70, § 9.
[99] *See supra* note 70, § 2.
[100] *Id*
[101] *See supra* note 70, § 7.
[102] *See supra* note 70, §. 7(2)(c) and (d).
[103] *Id*

Just like the US CAN-SPAM Act and the Australian Spam Act, the Singapore Spam Control Act also relies on an 'opt out' policy. Unlike the above mentioned Acts, the Spam Control Act prohibits sending of messages in bulk and not single unsolicited commercial electronic messages. The criterion enlisting bulk messages has been laid down in the Act and also discussed earlier. Following the Australian precedent the Act also applies to messages having a 'Singapore Link' the requirements for which have been given above. Since the Act came into effect only from 2008, thus there is a dearth of significant case laws in this regard.

SPAM -AN INDIAN PERSPECTIVE:

Indian companies are no strangers to spam. Spam equally poses to be a nuisance as much for Indian corporations and individual internet user as much as it is for foreign corporations and internet users, so much so that large organizations with more than 500 employees are willing to shell out anywhere between Rs. 1000-1200 per user to curb spam.[104] It has also been reported that 65.73 percent of Indian e-mail traffic accounts for spam.[105] Indians not only happen to be victims of spam but also one of the top originators of spam. [106]Indian are the second most spam originator worldwide, with 10.98 per cent of spam being sent globally from Indian IP addresses, according to a study.[107]

There is a lack of any comprehensive legislation covering spam in India which is fact also acknowledged by the Delhi High Court in the case of *Tata Sons* v. *Ajay Kumar Gupta*.[108] The case was wherein Tata Sons Ltd on behalf of VSNL filed a suit against the said defendant for transmission of spam. The Delhi High Court while issuing a first ever order of its kind in India restrained McCoy Infosystems and its proprietors and agents from "*causing transmission of unsolicited bulk electronic mail*" to any user of the services of an Internet Services Provider (i.e VSNL) or indulging in the activity of jamming the VSNL Internet server. The suit was one where it was asserted that through the Unsolicited Bulk Commercial E-mail McCoy Infosystems

[104]*See* Atanu Kumar Das, *India Inc. declares war on spam, at* http://www.expresscomputeronline.com/20050425/antispam01.shtml (last visited Mar. 26, 2010)
[105]*Id*
[106]*See India almost tops as world's spam HQ,*THE FINANCIAL EXPRESS, Mar. 25, 2010, available at http://www.financialexpress.com/news/India-almost-tops-as-world-s-spam-HQ/595502/ , (last visited Mar. 26, 2010)
[107]*Id*
[108]Suit No. 2158 of 2003.

Pvt Ltd and the other defendants were intentionally "trespassing" on VSNL's property despite being black-listed for habitual transmission of unsolicited commercial electronic messages in bulk.[109] It was held that in the absence of statutory protection to check spam mails on Internet, the traditional tort law principles of trespass to goods as well as law of nuisance would have to be used.[110] Even though the order passed by the Delhi High Court was only a temporary order, nevertheless the order is very much significant in many respects. Firstly, it recognizes that spamming is a problem and needs regulation, and secondly, in the absence of a specific law, judicial recognition through interpretation of other laws may be necessary.[111]

The above mentioned case has only happened to be a one-off case and the Indian courts are yet to address the issue in a substantial manner. Such cases can only provide a stop-gap solution to the menace of spam and the need for effective spam legislation is dire. The Information Technology Act, 2000 is the only statute that may somewhat have a thin linkage with unsolicited messages, though even though the Act itself lacks a specific provision putting a ban on spam. Section 67 of the Act regulates obscenity over the Internet and prohibits anyone from publishing or transmitting or causing to be published in the electronic form, any material which is lascivious or appeal to the prurient interest.[112]Thus the wording of this section would loosely bring spam under its ambit if the nature of such an electronic message is such that it is in the form of a pornographic message or which is derogatory in nature and not all forms of unsolicited commercial electronic messages. Thus it has to be said that in the absence of any statutory protection to check spam mails on Internet, it may be necessary to rely on the traditional tort law principles of 'trespass to goods' as well as the 'law of nuisance' to address the challenges posed by spammers.

On a closer look, until the enactment of spam specific laws in India, liability would continued to be brought under either tort principles of trespass to chattels, nuisance or criminal

[109]*See* Sreesanth, *Legal Aspects and implications of e-mail Marketing and Related Spam Laws, at* http://law4spamregulation.blogspot.com/2007/07/laws-for-spam-regulation.html, (last visited Mar. 26, 2010)
[110]*See* Rahul Dhonde, *Spam Is it time to legislate*?, *at*http://www.legalservicesindia.com/articles/spamli.htm, (last visited Mar. 26, 2010)
[111]*Id*
[112]S 67.**Publishing of information which is obscene in electronic form.** -Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeal to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

trespass u/s 441 of India Penal Code, 1860 (IPC) punishable u/s 447 of IPC.[113]Focusing on the tort of trespass of chattels, a chattel may be defined as an article of personal property.[114]Personal property, in turn, includes "everything that is the subject of ownership, not coming under denomination of real estate[115].In trespass to chattels the infringing party intentionally interferes with another person's lawful possession of a chattel.[116] The interference can be of any physical contact with the chattel, or any dispossession of the chattel. In order to establish this tort the plaintiff must prove that the defendant intentionally and without consent, physically interfered with the use and enjoyment of personal property in the plaintiff's possession, and the plaintiff was thereby harmed.[117] Therefore, included in a trespass to chattel cause of action is temporarily appropriating another's property for one's own use, such as where a spammer uses the equipment of another (e.g., ISP) to send email advertisements to its recipients (end users of ISP).[118]The intention being talked about here refers to the intent of making physical contact with another's possession and not the intent to trespass. Intention of spammer can never be put to question.[119] The reason why spammers bulk e-mails is so that they may reach the maximum number of users of an ISP. Since all e-mails are directed towards a particular destination (i.e. end user) en-route the server of the closest associated ISP thus contact with an ISP's server facilities is an inevitable consequence of mailing. Secondly, trespass to chattels also requires interference with the lawful possession of another's chattel. Such interference may take place either by dispossessing another of his chattel or by using or intermeddling a chattel in possession of another.[120]An outright dispossession of servers belonging to ISPs by spammers through spam mail is highly unlikely, what is possible however is intermeddling of a chattel.[121] It may be said that even though it is the ISP who owns the server as a whole which may be considered as its personal property, but when the end users signs a contractual agreement with an ISP to use his service then each such user is

[113] S441 **Criminal Trespass** - Whoever enters into or upon property in the possession of another with intent to commit an offence or to intim*Id*ate, insult or annoy any person in possession of such property, Or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intim*Id*ate, insult or annoy any such person, or with intent to commit an offence, is sa*Id* to commit "criminal trespass".

[114]Black's Law Dictionary (8th ed. 2004)

[115]*Id*

[116] W. PAGE KEETON, *et al.*, PROSSER AND KEETON ON THE LAW OF TORTS (5d ed. 1984).

[117]*Id*

[118] Anne E. Hawley, *Taking Spam out of your cyberspace diet: Common Law applied to bulk unsolicited advertising via electronic mail, 66 UMKC L. Rev. 381*(1997)

[119]*Id*

[120]*Id*

[121]*Id*

allocated some space on the ISP's server. The space allotted to each such user on the server of the ISP is exclusive to each user and can be called as the private space of such user which could be analogously compared to a license granted over real estate. Each such user has the right to access his e-mail in his personal account at speeds assured to him by the ISP. If the spammers clog up the limited private space of a user on the ISP's server with spam then the user would not be able to use such space as per his wishes. A user may also be forced to pay for unwanted data downloaded on account of spammers. Hence such an act may amount to intermeddling and thus fulfilling the requirement for establishing the tort of trespass to chattels.

Under the Indian Penal Code, 1860, a trespass may amount to criminal trespass if it is done with an intent to commit an offence, intimidate, insult or annoy the person in possession of property. Black's law dictionary defines annoyance as 'nuisance'.[122]Nuisance has been defined in Black's law dictionary as follows:

"*A condition, activity, or situation (such as a loud noise or foul odor) that interferes with the use or enjoyment of property; esp., a non transitory condition or persistent activity that either injures the physical condition of adjacent land or interferes with its use or with the enjoyment of easements on the land or of public highways. • Liability might or might not arise from the condition or situation.* — Formerly also termed annoyance.[123]"

A close reading of S 441 of IPC 1860 "Whoever enters into or upon property in the possession of another…." brings this fact to light that the section is to be narrowly interpreted as compared to the tort of trespass. The criminal provision of trespass particularly focuses on an individual entering into or upon property in the possession of another person. In cyberspace it is only a spam message that is entering into the private property of the ISP and not the spammer himself. In contrast, the tort law principle of trespass of chattels is quiet broad and covers 'interference with the lawful possession of property". Such interference can also be on account of conduct of a person and not necessarily through his physical presence which is the essence of the criminal provision for trespass. The spam messages being sent to the private space of an end user of an ISP may pose to be a hassle in his right to use or enjoy his property i.e. the email account belonging exclusively to the user over the server of the ISP. Thus it is not the spammer himself

[122]*See supra* note 114.
[123]*Id*

but the spam messages that pose to be an annoyance, through the conduct of the spammer. Hence, in my opinion sending of spam will not attract liability under IPC provision of criminal trespass but only under tort of trespass.

Expanding further over the tort law concept of 'nuisance'. As has already been elaborated, the definition of nuisance[124] makes it nothing more than an extension of the second requirement of trespass of chattels. It is essentially nothing more than interference with the lawful possession of property of another by intermeddling particularly in the case of sending spam messages. Thus the clogging up of the exclusively allotted personal space of end-users over the servers of ISP with spam messages will only pose a hassle for such users who might face reduced performance of ISP services or may be forced to pay for downloading unwanted spam messages. Hence such a conduct on part of spammers of sending spam messages will also pose to be a nuisance under tort law.

Under section 292[125] of IPC the selling, making available for hire of obscene books, pamphlets etc is prohibited. Section 293[126] is similar to the above mentioned children and applies

[124] *Id*

[125] **Sale, etc., or obscene books, etc.**(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

3[(2)] Whoever-

(a) Sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or

(b) Imports, exports or conveys any obscene object for any of the purposes aforesaid or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) Takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) Offers or attempts to do any act which is an offence under this section,

Shall be punished 4[on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees].

5[Exception-This section does not extend to-

(a) Any book, pamphlet, paper, writing, drawing, painting, representation or figure-

where such a sale or hire is made to young children. The wordings used in the above mentioned two sections are similar to that used in S 67 of IT Act, 2000. However the IT Act deals with such publishing in electronic form and this pegs the question whether publishing of such obscene material in electronic form can attract liability under the IPC. Upon the enactment of the IT Act, some amendments were also made to the IPC with one of them being the incorporation of S 29A in IPC after S 29. Section 29[127] describes document and S 29 A gives the definition of electronic record as given in the IT Act, 2000. As per its definition any matter expressed over any substance is a document, and quiet certainly S 292 would apply over matter described in S 29. So the question is whether matter published in electronic form would be considered as a document? It is submitted that such matter present electronically cannot be considered as a document in context of IPC. During the enactment of IT Act amendment was made to incorporate the definition of 'electronic records' into IPC and it is the publishing of obscene form of such electronic records which is punishable under S 67 of IT Act. This section is a penal provision and makes for a punishment of 5 years. Hence by also implicating electronic records to be read under section 292 of IPC there would be two penal provisions for the same offence under two separate statues which would lead to multiplicity of legal provisions, which was originally never the intention of the legislators. If the legislators wanted electronic records to be brought under the ambit of S 292 then the necessary amendment would have been made to the definition of document in S 29 itself to expressly demonstrate such an intention. However they chose not to do so as such act was already covered under S 67 of the IT Act which also happens to be a penal

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art of learning or other objects of general concern, or

(ii) Which is kept or used bona f*Id*e for religious purposes;

(b) Any representation sculptured, engraved, painted or otherwise represented on or in-

(i) Any ancient monument within the meaning or the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

(ii) Any temple, or on any car used for the conveyance of *Id*ols, or kept or used for any religious purpose.

[126]**Sale, etc., of obscene objects to young person** - Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished 2[on first conviction with imprisonment of either description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees

[127]**Document** - The word "document" denotes any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter.

provision. Thus the act of sending spam messages may attract liability under S 67 as has been already discussed but not under S 292 or 293 of IPC.

In the end, it would be suffice to say that the need for a spam legislation for regulating this menace is dire. Following the international precedents of enacting of spam legislations we need a spam specific legislations to remove the ambiguities which may arise while imposing liability through various tort law concepts.

CONCLUSION:

Unsolicited Commercial Electronic Mail remains undesirable for several reasons. However to sum up, spam or unsolicited commercial electronic mail generally contain useless information that one never needs, or market products that one may not require. Spam mails also prove to be a constraint on resources of ISPs as they take up valuable space and pose to be a nuisance for the common internet user as one needs to pay for the internet usage and downloading of unnecessary data; also, piling up of such mail on the servers of ISPs results in slowing of speeds and degradation of performance. This may force the internet users to look for alternatives.

Various tort law concepts of trespass to chattels and nuisance have been applied by courts in the absence of any statutory regulation. The concept of trademark dilution may also be extended to sending spam using the domain name of some trademarked entity by spammers. However considering the extent and nature of the problem (as evident from the statistics) which is only going to increase in the near future, both in India as well as globally, it would only be wise to enact a legislation regulating this menace as has been done by many of our peer nations who happen to be at the forefront of technology.

An analysis of various municipal legislative provisions on spam suggests that they regulate and not prohibit the sending of spam. It is only the sending of unsolicited electronic messages which are of commercial nature that are banned and not all forms of unsolicited nature. This is done to balance the conflict of interest of both the senders of such messages and their recipients. On the whole, the basic features of all spam legislations are the same, i.e. pursuance of an ‘opt in’ or ‘opt out’ policy, prohibition of sending of messages with false or deceptive

headers making it mandatory to mark the messages with some information so as to disclose the identity of the sender and in some other cases, an additional feature being present that the message should possess a local or country link e.g. Australian link, Singapore link. India should be no exception and in line with the legal developments worldwide, should contemplate the enactment of a spam specific legislation. Time and again, it has been argued that a separate legislation may not always be the correct approach to the problem. While this may hold good in some cases, issues such as the present one are unique in terms of age-old understanding of infringements, invasions and violations and the means of commission. The technological intricacies involved, the underlying purposes and perspectives and the trans-boundary nature requisitions a nobler and variant policy making that may work best in the circumstances.

The instances of spam being reported have been very few in India but this is not to say that the spread of the problem is of no concern here. Statistics speak for themselves with India not only being one of the topmost originators' of spam but also a victim of this menace. The concept of maintaining 'blacklist' and 'whitelist' should be borrowed from the practices of American ISPs and be given the force of law in its implementation in India. If it is so then it will only be more convenient to put a check on both spam as well as spammers and at the same time take care of innocent mail senders. Secondly, whether India should follow the much touted 'opt out' policy pursued by USA and Australia or the stricter 'opt in' policy followed in EU is open for debate. However as far as any of them is pursued it will definitely be in the interests of the Indian Internet users as the objective of both is the same , that being to prevent unsolicited commercial electronic messages from reaching the users. However in a contrast to the US legislations I believe that power should also be given to individual users to bring about action otherwise the reporting and prosecution of spam related cases will only be low which is what the present scenario is. Also, the cyber crime cells of various state police departments seem to be the only relevant authorities which should have jurisdiction over such matters and be empowered with enforcing the Act. There should also be an outright ban on use of dictionary and address harvesting software for their use of sending spam messages alongwith prohibiting of sending messages with deceptive headers. Some states consider sending of a single message as spam while others (e.g. Singapore) consider sending of bulk messages (atleast 100) as spam. The number of messages sent for them to be considered as spam is a big controversy as in the above case if spammers purposefully send 93 or 94 messages with the purpose of defeating the

statutory bar would that also amount to sending of spam. I also personally favour the latter approach of considering messages as spam only if a certain number of messages are sent but also believe that the number of bulk messages sent should be reduced to about 30. It would also be preferable if the provision regarding the same is an open ended one with the courts being expressly given the discretionary power to consider some messages which fall short of the statutory bar but sent with the purpose of defeating the same to be considered spam. Lastly the unsolicited commercial messages sent should also contain an 'Indian Link' and that being that the messages must originate or be sent from a server in India; or the senders of message be in India; or the message must be delivered in India.

It has to be said that the subject of unsolicited commercial electronic message is very important in the current scenario which has been displayed by the urgency with which many of the leading countries of the world have enacted their own spam specific statutes. Considering the rise of India in the Information Technology sector it is worth mentioning that our country also requires such a legislative measure to counter this ever growing menace of spam. The industry leaders today who use cutting edge technology to compete with competitors from around the globe cannot afford to waste time on the nuisance posed by unsolicited commercial electronic messages or spam, and therefore we require our laws to take effective measures to neutralize this problem.

IJMRA