Spam – *A new bug in town*

by Banerjee Soumya.[1]

The Internet's explosive growth has opened new avenues for communication, learning, commerce and entertainment. Like any new medium, however, it comes with its share of problems. Since, one of the most widely used functions of the Internet is e-mail, it is estimated by one survey that by the end of 2005 the number of e-mails sent in any average day is expected to exceed 36 billion.[2]

However, in recent times it has been observed that, although the purpose of the e-mail is to make communication more convenient, e-mail does not always provide the desired efficiency.[3]

Much of the inefficiency problem with e-mail can be attributed to the increase in the number of advertisers using the Internet. The attempt of the advertiser's to capitalize on the seemingly endless pool of potential customers on the internet has created nightmares for individual consumers, business organizations and internet service providers. The nightmare comes in the form of spam.[4]

Spam, which in a more refined way is called as Unsolicited Electronic Mail, has traditionally been viewed mainly as a nuisance, but it also constitutes a security threat. Three general categories of approaches have been used to address the spam problem: (1) informal measures, such as social norms and self regulatory efforts, (2) technical measures undertaken by individuals and organizations and (3) legal responses.

Why Spam is a Problem

Objectionable Content: Spam is problematic for a number of reasons. Many of the objections to spam relate to its content. For example, some object to receiving commercial messages, particularly those that promote questionable ventures, illegal business schemes and marketing scams. Others are offended by messages that contain or advertise sexually explicit material. Such messages are particularly troubling when they are sent to minors. Senders of unsolicited messages rarely know the age of persons to whom the messages are sent.[5]

Consumption of Internet Resources: Spam represents a significant proportion of all e-mail traffic, consuming massive amounts of network bandwidth, memory, storage space, and other resources. Internet users and service providers spend a great deal of time reading, deleting, filtering, and blocking spam, so Internet users pay more for Internet access as a result of spam.[6] Large Internet Service Providers (ISPs) such as American Online (AOL) report that anywhere from one-third to two-thirds of their email server capacity is consumed by spam.[7]

---

[1] **Banerjee Soumya** (B.Sc. LL.B.) is an Associate of Saha & Ray. He may be reached at soumya.banerjee@saharay.com

[2] Cindy.M.Rice, 'Comment: TCPA- A Justification for Prohibition of Spam?', *North Carolina Journal of Law & Technology*, Volume 2 ,Issue 3, Spring 2002, at http://www.spamlaws.com/articles

[3] *ibid.*

[4] *Also see: CompuServe Inc. v. Cyber Promotions Inc.* (S.D. Ohio 1997) 962 F. Supp. 1015, 1018 n.1 - [The term Spam] is derived from a skit performed on the British television show *Monty Python's Flying Circus*, in which the word 'spam' is repeated to the point of absurdity in a restaurant menu.

[5] *Also see*: David E. Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail" (2001) 35 U.S.F. L. REV. 325, at http://www.sorkin.org/articles/usf.pdf

[6] *ibid.*

[7] *Also see*: http://news.yahoo.com/news?tmpl=story&u=/cmp/20040526/tc_cmp/21100194

Threat to Internet Security: Spam is both a wasteful activity and one that poses a threat to the security and reliability of Internet communications. Many spams come with hostile file attachment or embedded code which may pose security threat. An example of this would be the large scale disruptions of computer networks all over the world caused by a spammer virus called "*Melissa*" which attacked Microsoft's operating systems.[8]

Legal Action Against Spamming

In the United States, there are specific anti-spamming legislations, at both Federal level and State level which can be used by ISPs to obtain relief. But, in India the recently enacted Information Technology Act does not specifically deal with spamming (Section 66& 43(e). Therefore, the only forms of relief that subscribers and ISPs in India can find currently, are in tort theories, trademark law and criminal law.

Application of Tort principles to counter spam

A tort is a breach of some duty independent of a contract-giving rise to a civil cause of action and for which compensation is recoverable.[9] The principal aim of tort law is compensation of victims or their dependants.[10] One of the tort principles namely "Trespass to personal property" can be and has been used to counter spam.

Trespass to chattels is committed when a person uses or intermeddles with another's personal property without authorization. The trespasser is liable to the rightful possessor of the property if the property's value or condition is impaired, or if the possessor is deprived of its use for a substantial time.[11] Under this theory, the defendant becomes liable for trespass when the defendant's use or contact materially harms the quality, physical condition, or value of the possessor's chattel.

Internet Service Providers have a possessory interest in their chattel or personal property i.e. their computer equipment and software. This possessory interest is affected when a spammer, without authorization, transmits spam mails through the ISP's server. Because those spam mail clogs the server of the ISP, the server gets slowed down, and as a result the quality or value of the possessory interest gets diminished.

Case Study: The famous case of *Compuserve v. Cyber Promotions*[12] serves as an ideal example to demonstrate how ISPs can use the trespass to chattel theory to sue spammers. In Compuserve, an ISP brought a trespass to chattels action against Cyber Promotions, a company notorious for its spamming activities. It was determined that Cyber Promotions had intermeddled with Compuserve's possessory interest in its computer equipment by its unauthorized and intentional use of the ISP's equipment to send unsolicited commercial e-mail.[13] The court found that the harm resulting from Cyber Promotions' intermeddling was a decrease in the value the ISP placed on its equipment to serve its subscribers. Specifically, the court explained that '*although*

[8] *Also see*: Andrew Brown, "Micro Organism (Spamming)" (9th April, 1999) *NEW STATESMAN*, http://www.internetwk.com/story/INW19990402S0003
[9] *Also see*: Ratanlal & Dhirajlal, *Law of Torts* (1999) page 4.
[10] *ibid.* page 5.
[11] *Also see*: *Am. Online Inc. v. LCGM Inc.*, 46 F. Supp. 2d at 451–52.
[12] *Also see*: 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).
[13] *ibid.*

spamming did not physically damage the ISP's equipment, the value of the equipment was still diminished because the ISP was unable to access the resources necessary for efficient provision of services to its subscribers'[14].

Furthermore, the court noted that the strain placed on plaintiff's resources resulted in a loss of revenue due to unsatisfied customer subscription cancellation, causing harm to Compuserve's business reputation and "goodwill," which is also actionable under the trespass to chattels doctrine.[15]

Action Under Trademark Law: Trademark law is designed to secure to the owner of a trademark, the goodwill of his/her business. Internet Service Providers (**ISP**), such as American Online (**AOL**) and Compuserve, often incorporate their trademark name within their Internet domain names. Spammers often enter false return addresses in the messages they send and sometimes even go so far as to enter the name of an ISP in order to avoid receiving rejected mail or requests to cease and desist from subscribers. If a spammer uses such a domain name in conjunction with its own advertising service in a manner that causes confusion as to the origin of its service, the spammer may be liable for trademark infringement or fraud.

Similarly, if a spammer uses an ISP's domain name trademark in a manner that results in the "dilution of the distinctive quality" of the mark, the spammer may be liable for trademark dilution. However, in order to succeed in a trademark dilution claim, a trademark owner must show that he owns a famous and distinctive mark and that the alleged use of the mark is likely to result in its dilution through blurring or tarnishment.

Case Study: America Online Inc v. IMS[16] - This case is an example of how principles of trademark law could be successfully applied in a case of spamming. In this case, the plaintiff, an ISP successfully brought suit against a spammer using the principles of trademark law. AOL, the plaintiff ISP successfully brought false designation of origin and trademark dilution actions against IMS, an electronic marketing company. AOL alleged that the defendant improperly sent over 60 million unauthorized e-mail messages to AOL subscribers. The court held that defendant's act of forging "aol.com" in the headers of his e-mail constituted both a false designation of origin and dilution in violation of federal trademark law.

This conduct constituted false designation of origin because *any e-mail recipient could logically conclude that a message containing the initials "aol.com" in the header would originate from AOL's registered Internet domain and thereby be deceived into thinking that AOL sponsored or approved of defendant's bulk mailing activities*. This injured AOL's reputation with its subscribers.[17]

Criminal Trespass Under Indian Penal Code: Apart from remedies under Tort & Trademark Law there is a possibility of spamming being brought within the purview of Section 441 of the Indian Penal Code (**IPC**), 1860, which deals with Criminal trespass. Section 441 of the IPC states that, *Whoever enters into or upon property in possession of another with an intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains therewith intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass".*[18]

---

[14] *ibid.*
[15] *ibid.*
[16] *See*: 46 F. Supp. 2d 444.
[17] *ibid.*
[18] *See*: Section 441 of Indian Penal Code.

It is submitted that action can be taken against a spammer under the provisions of this section because to disseminate spam, a spammer will have to use the server of the ISP, and therefore the ISP may be "annoyed" by the misuse of his property and thus it could constitute "criminal trespass" within the meaning of Section 441 of the IPC. However, since in India, till now there is hardly any case on spamming, so there is no case law where the Court has allowed an action of criminal trespass under section 441 of the IPC against a spammer. Apart from the abovementioned forms of relief, section 66 and 43 (e) of the Information Technology Act, 2000, may also help Internet Service Providers to fight against spamming. Section 66 of the Information Technology Act primarily deals with hacking. However, it has been defined that, hacking in such a wide way may be applied in cases of spamming also. The Section states that; *Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking*"[19]

By including the phrase *diminishes its value or utility* the legislators may have unknowingly made this section applicable to cases of spamming also. It has been discussed earlier in the Compuserve's case[20] that the transmission of unsolicited e-mails and the resultant clogging of the entire server of the Internet Service Providers, although do not damage the server physically but certainly diminishes its value or utility. So, by that principle since the action of the spammers diminishes the value of the computer resource of the ISPs, as per Section 66 spamming could also be termed as hacking. Although this is theoretically possible but whether it will be applied in practice would depend upon what interpretation the Courts give to the word "*its*" in the Section. This is because if the word "*its*" within the phrase *diminishes its value or utility* means or qualify the *computer resource* then this section can be applied to spamming. However if "*its*" means or qualify *the information residing in a computer resource* then this section can not be applied to cases of spamming, since in cases of spamming the information stored in a computer system does not get affected.

Section 43(e) of the Information Technology Act, 2000 may also be applied to cases of spamming. This section says that – "*if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network disrupts or causes disruption of any computer, computer system or computer network he shall be liable to pay damages by way of compensation not exceeding* one hundred lac rupee *to the person so affected.*"[21] It is submitted that since spamming slows down the server of the ISPs and hampers its normal working and also since no ISP expressly authorizes a spammer to send spam mails through its server, so it can be said that the sender of spam mails causes disruption of the Computer Network of the ISPs within the meaning of section 43(e) of the Information Technology Act. Thus this section can be interpreted in this way to make a spammer liable to pay damages to an ISP.

Conclusion: Spam presents a dangerous threat to the efficiency and cost effectiveness that has made e-mails so popular among individuals and corporate world as a major source of communication.[22] Neither technical measures nor self-regulation or other informal measures have succeeded in solving the problem of spamming. So now it is up to legal approaches to end this menace. In this document two basic types of legal approaches has been discussed - legislation & litigation. Countries like USA, UK, Italy,

[19] *See*: Section 66 of Information Technology Act, 2000.
[20] *See*: 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).
[21] *See*: Section 43 of the Information Technology Act, 2000.
[22] SPAM – It's not Just for Breakfast Anymore: Federal Legislation and the Fight to Free the Internet From Unsolicited Commercial E-Mail, Gary S. Moorefield at www.bu.edu/law/scitech/volume5/5bujstl10.pdf

Germany, Austria, etc have specific anti –spam legislation in place to deal with problem. These legislative responses to spam, ranges from mere disclosure requirements to outright prohibition of unsolicited bulk or commercial e-mail messages. For example, in the United States, Delaware has enacted what appears to be the most restrictive spam law.[23] As per this law, sending of any unsolicited bulk commercial e-mail is an offence. The European Union does not prohibit unsolicited commercial email, but permits individual member states to do so. Finland, Germany, and Italy all have laws prohibiting Unsolicited Commercial E-mails, while Austria prohibits both Unsolicited Commercial E-mails and Unsolicited Bulk E-mails.[24]

Apart from enacting legislations which specifically deal with unsolicited e-mails, litigation is the other method to deal with spamming. The two legal principles which are frequently used in cases filed against spammers are – trespass to chattel & trademark dilution. However, litigation has its well known drawbacks – firstly it is time consuming & secondly, it is quite expensive. For this reason, litigation may not be always an ideal choice for fighting spam. For countries like India however, where till date there is no specific anti-spam legislation, litigation remains the only option. In this respect it is important to mention the recent interim order (final order is awaited) of the Delhi High Court, which must be the first-ever judicial order in India on the issue of spam. In the case of *Tata Sons v. Amait KumarGupta*, Justice R.C. Chopra has passed an interim injunction against McCoy Infosystems Pvt Ltd restrained it from *causing transmission of unsolicited bulk electronic mail* to any user of the services of VSNL Internet server.[25] A suit was instituted by Tata Sons, on behalf of VSNL, wherein it was alleged that through the Unsolicited Bulk Commercial E-mail (**UBCE**), McCoy Infosystems Pvt Ltd were intentionally "*tresspassing*" on VSNL's property despite being black-listed for habitual transmission of UBCE.[26] The interim order of the Delhi High Court is significant because firstly, it recognizes that spamming is a problem and needs regulation, and secondly, it lays down that in the absence of a specific law, judicial recognition through interpretation of other laws is necessary.

End.

[23] *See*: David E. Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail", 35 U.S.F. L. REV. 325 (2001), at http://www.sorkin.org/articles/usf.pdf.
[24] S*ee*: EuroCAUCE, *at* http://www.euro.cauce.org/en/countries/c_it.html
[25] *See*: Azmul Haque & Ajay Shaw, SPAM & Indian Legal Position , Economic Times, 15th February, 2004.
[26] *ibid.*