IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12803

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Spim, Spam and Advertisement: Proposing a Model for Charging Privacy Intrusion and Harassment

Dionysios Politis, Dept of Informatics, Aristotle University of Thessaloniki, Thessaloniki, GR-541 24, GREECE, T: +30 2310 998412, F: +49 2310 998419, dpolitis@csd.auth.gr

Georgios John Fakas, Dept of Computing & Mathematics, Manchester Metropolitan University, Chester Str, Manchester, M1 5GD, UK, T: +44 161-2473537, F: +44 161-2471483, g.fakas@mmu.ac.uk

Konstantinos P. Theodoridis, Centre of International & European Economic Law, Ikaron 1, Thessaloniki, GR-541 02, GREECE, T: +30 2310 486900, F: +30 2310 476 366, kostistheodoridis@gmail.com

ABSTRACT

An issue factually challenging the peer-to-peer nature of the Internet is the increase of spam trafficking. Having reached record levels at the beginning of this year, it raised consciousness that Internet communication was endangered by an erosive threat similar to the uncontrollable, massive free circulation of MP3s that devastated the musical industry. Recent combined advances in the software industry and in the legal front have reduced the phenomenon. The technical, social, financial and legal parameters of this campaign are examined in this paper under the prism of a networked economy.

INTRODUCTION

A significant problem of our times, accelerated by the advances in technology, is the plethora of commercial Internet messages usually defined as *spam*, while the equivalent in classic television emission is the frequent and uncontrollable advertisement. Advertisement, perceived as an expression and factor of the economy, is legitimate and desirable. However, abusive advertising practices cause multipledamage: invasion in our private communication space, homogenisation of morals and customs leading to globalized overconsumption. Variations and cloning of spam and advertisement include *spim*, distributed instant messaging using bulk *SMS*'s over mobile telephone networks or the web, wireless attacks and penetration, targeted unsolicited online harassment and others.

PROBLEM FORMULATION

Spam is usually defined as "unsolicited bulk e-mail". This is generally done for financial reasons, but the motive for spamming may be social or political. Unsolicited means that the recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content (Cheng, 2004).

Rough estimates conclude that e-mails like "Buy this product" or "Participate in this campaign" are more than 60% of what is the normal daily load (Doyle, 2004). Generally, the longer an email address has been in use, the more spam it will receive. Moreover, any email address listed on a website or mentioned in newsgroups postings will be spammed disproportionally. Mailing lists are also a good target.

A variation of spam is *spim*. It is defined as unsolicited commercial messaging produced via an instant messaging (IM) system. It disperses messages to a pre-determined set of screen names, which are generated randomly or are harvested off the Internet.

Spam as a social phenomenon arises from an on-line social situation that technology created. First, it costs no more to send a million e-mail messages than to send one. Second, hits are percentage of transmissions, so sending more spam means expecting more profit (Whitworth, 2004). So, from the advertising point of view, the important characteristic of spam is that it is practically with no charge. It is not the best e-mail communication technique, it is not the most efficient but it attracts people because of its free ride.

LEGAL ASPECTS OF SPAM

USA

Since 1996 many cases[1] between Internet Service Providers (ISPs) and spammers found their way to the court; however the problem has always remained the same: lack of specific legal regulation, which led to objectionable decisions (Frank, 2003, Kasprzycki, 2004). The need for an ad hoc federal law was obvious and after many rejected drafts, on 01.01.2004, the "CAN SPAM Act 2003[2]"was finally put into force. This Act includes a variety of measures for the prevention and the restriction of the problem and provides serious penalties for the spammers. More specifically, among others:

- spammers face penalties of imprisonment up to 5 years and/or high fines.
- the falsification of the sender identity or header information, the harvesting of electronic addresses and the unauthorized manipulation of computers and servers is penalized (Sec. 4).
- advertisers are obliged to include an "Opt-out" option in each advertising e-mail (Sec. 5).
- e-mail advertisements must be labelled as such, with the addition of the abbreviation "ADV" in the line of subject (Sec. 11).
- the formation of a "Do-Not-E-Mail registry" is foreseen (Sec. 9)[3], where the internet users can register themselves in order to avoid receiving advertising e-mails. Advertisers owe, theoretically, to consult this list before launching a mass electronic advertising campaign.

EU

European Union has demonstrated its prompt reflex as far as the protection of European consumers is concerned, by publishing the Directive 1997/7/EC "on the protection of consumers in respect of distance" and preventing the use of certain means of distance communication (telephone, fax), without the prior consent of the consumer

(Art. 10). Later on, the Directive 2000/31/EC "on electronic commerce" focused further on the unsolicited commercial electronic communication prescribing the formation of opt-out registers (Art. 7). Finally the Directive 2002/58/EC "on privacy and electronic communication", replacing the Directive 1997/66/EC, is providing a powerful legal tool against spamming. According to article 13 of the new Directive:

- the communication for the purpose of direct marketing via telephone, fax or e-mail requires the prior consent of the consumer-user (opt-in) or is acceptable in the context of the sale of a product or a service (soft opt-in).
- each advertising e-mail must incorporate an easy and costless "opt-out" opportunity for the recipient in order to object to such use of electronic contact details.
- disguising or concealing the sender identity and providing an invalid reply address for the opt-out, shall be prohibited

Nearly all member states have already adjusted the national legislation and have established regulatory authorities like OPTA[4], that has issued its first fines[5].

CHARGING SPAM

Estimations and Projection

In order to propose a model for charging spam, the authors of this article conducted a survey on spam. The graphical outputs of the survey can be seen in Fig. 1.[6] For 8 months 16.478 active e-mail accounts where monitored, not of course on their content, but on their reaction to spam as far as an anti-spam filter was concerned, applied at the e-mail server's level. For legal reasons having to do with the protection of personal data, it was not possible to estimate the filtering strength of the software devices that end users deploy themselves at their e-mail clients.

Charging Spam: A Calculus Analysis

Suppose that there are n potential spammers, indexed by i = 1, ..., n. Each of them transmits q_i packets to the Internet, so the aggregate number of transmitted packets in a given period is $Q \overset{def}{=} \sum_{i=1}^{n} q_i$. The network is supposed to have a limited capacity, denoted by $\bar{Q}$, which is measured not in communication terms, since the present Gigabit Ethernet does not seem to congest from text messages, but from user dysphoria, caused by imponderable and excessive spam.

Consumers gain utility by communicating via the net, with e-mails, and gain disutility most of their communication is spam, i.e. noise, intrusion or harassment.

In this case, there is a price p per transmitted packet, whether this is charged a-priori, as a preventive measure, or afterwards, as and *ad-hoc* fine[7].

Therefore, the utility function of each consumer is defined as follows (Shy, 2001):

$$U_i \overset{def}{=} \sqrt{q_i} - \delta \frac{Q}{\bar{Q}} - pq_i = \sqrt{q_i} - \delta \frac{\sum_{j=1}^{n} q_j}{\bar{Q}} - pq_i \qquad (1)$$

where $\delta > 0$ measures the intensity of disutility caused by spamming. The "latency" caused by the spam effect is measured by $Q/\bar{Q}$ which is the ratio of actual, non infected by spam, e-mail communication capacity. If $Q < \bar{Q}$ the network is not congested by spam. If, however, $Q > \bar{Q}$ the network bristles with spam and user discontent increases.

Since each consumer participates as a peer in this communication, (s)he takes the network usage by other consumers $\sum_{j \neq 1} q_j$ and chooses his/her usage q_i that solves

$$\max_{q_i} U_i = \sqrt{q_i} - \delta \frac{q_i + \sum_{j \neq 1} q_j}{\bar{Q}} - pq_i \qquad (2)$$

yielding that the first and second order derivatives, regarding the transmitted packets q_i for maximum conditions are given by

$$0 = \frac{\partial U_i}{\partial q_i} = \frac{1}{2\sqrt{q_i}} - \frac{\delta}{\bar{Q}} - p \quad \text{and} \quad \frac{\partial^2 U_i}{\partial (q_i)^2} = \frac{-1}{4\sqrt{(q_i)^3}} < 0 \qquad (3)$$

Hence, the individual and aggregate packet transmission levels are

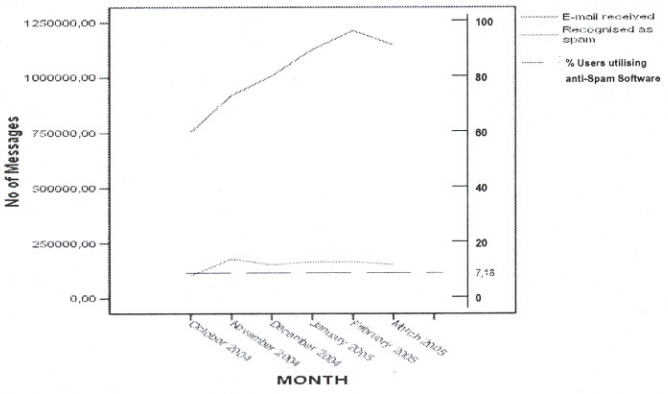
$$q_i = \frac{\bar{Q}^2}{4(\delta^2 + p^2 \bar{Q}^2 + 2\delta p \bar{Q})} \qquad (4)$$

Example:

Suppose that a spammer sends spam messages to the 16.478 active e-mail users of the Aristotle University of Thessaloniki (AUTh). – a message per day, for one month. It has been estimated for theses users that they accept on average 1.064.573,286 messages per month (see Fig. 1), therefore the distribution of messages per user for one month interval is 1.064.573,286 / 16.478 H" 65 messages.

The e-mail capacity of the server is not limited however to only 1.000.000 e-mail messages per month. AUTh hosts about 50.000 students, researchers and employees. The average world user is considered to send and receive about 200 messages per month. So, the system would be saturated if all 50.000 users were sending and receiving e-mails, i.e.

Figure 1. Spam trafficking at AUTh (Aristotle University of Thessaloniki). Blue line: the e-mail messages that AUTh's 16.478 active users received. Green line: the number of e-mails diagnosed as spam by the Spamassasin® software. Red line: the percentage of active users deploying the Spamassasin filtering mechanism.



$$\bar{Q} = 200 \text{ x } 50.000 = 10.000.000 \quad (7)$$

Hence, solving equation (5) we have that

$$\delta = \frac{\bar{Q}}{2\sqrt{q_i}} = \frac{10.000.000}{2\sqrt{64,61}} = 622.042,6 \quad (8)$$

Solving equation (4) for p yields p= 0,001 L per every spam message sent.

Accordingly, we deduce that if detected and litigated, the spammer should be charged with p = 0,001 L per spam message, that he would be charged for 16.478 x 30=494.340 illegally sent messages. These sum up for 494. 340 x 0,001 = 494,34 L.

This amount is roughly equivalent with the cost of advertising for a month to the campus with any other method, like say, distributing leaflets, having in mind of course that statistically only 1‰ of the spam recipients correspond to the advertiser, i.e. 1‰ x 16.478 = 16 individuals!

EPILOGUE AND CONCLUSIONS

The combined action of substantial legal countermeasures and advanced techniques of content filtering have limited the exaltation of spam.

The spam issue is part of a more complex phenomenon concerning the governance of the Internet, the economics of networked industries, technological advances and software development.

The spam issue does not merely threaten the future of a self governed Internet; it tests the tolerances of many factors for the networked economies. Therefore, justified legal action should be enforced.

REFERENCES

Cheng, T. (2004): Recent international attempts to can spam, *Computer Law & Security Report*, Vol. 20, no. 6, pp. 472-479.

Doyle, E. (2004): Spam rules - and there's nothing you can do, *Elsevier Infosecurity Today,* November/December, pp.24-28.

Frank, T. (2003): Zur strafrechtlichen Bewältigung des Spamming, p. 177.

Funk, A., Zeifang G., Johnson D. T., Spessard R. W. (2003): Unsolicited Commercial E-mails in the Jurisdictions of Germany and the USA, *CRi* 5, p. 141.

Kasprzycki, D. (2004): Trends in regulating Unsolicited Commercial Communication, *CRi* 3, p. 77.

LeClaire, J. (2004): Netherland issues its first fines against spammers, *e-Commerce Times,* 29.12.2004.

Shy, O. (2001): *The Economics of Network Industries,* Cambridge University Press.

Whitworth, B., Whitworth, E. (2004) :Spam and the Social-Technical Gap, *IEEE Computer*, Vol. 37, No. 10, pp. 38-45.

ENDNOTES

1 E.g. America Online Inc. v. Cyber Promotions Inc. (E.D. Pa. 1996), CompuServe Inc. v. Cyber Promotions Inc. (S.D. Ohio 1997), Hotmail Corp. v. Van$ Money Pie Inc. (N.D. Cal. 1998), America Online Inc. v. LCGM Inc. (E.D. Va. 1998).

2 *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, 15 U.S.C.A. § 7701-7713.

3 See further analysis by Funk, 2003.

4 OPTA, Netherland's Independent Post and Telecommunications Authority. http://www.opta.nl.

5 E.g. US$ 61.000 against an individual, who was involved in four spam campaigns, US$ 34.000 against a company spamming about financial software, $27.000 against a company sending spam text messages on mobile phones (LeClaire, 2004).

6 Statistical data from a survey conducted at the Network Operations Center (NOC) of the Aristotle University of Thessaloniki (AUTh) from 1.10.2004 till 30.4.2005.

7 See *supra note* no. 4.