Service Provider Responsibility for Unsolicited Commercial Communication (Spam)

Evangelos Moustakas, Penny Duquenoy
School of Computing Science, Middlesex University, London, UK.
{e.moustakas, p.duquenoy}@mdx.ac.uk

Abstract. The Internet introduced the concept of email – a means of communication that arguably provides the communication base for industry in the developed world. Advertisers have not been slow to take up the opportunities offered by the Internet and the World Wide Web – in many cases subsidising web-site presence. Advertising has its place, however, and many would argue that one of the less popular side effects of fast, easy and global communication has been the exploitation of this medium for sending 'spam' (or junk-mail). The focus of this paper is on the role of Internet Service Providers (ISP's) as the principle gate-keepers between the Internet and email-users. Legislation recognises this role and addresses the problem of spam. Other approaches to tackle the problem come from self-regulation and software applications (filtering technologies). This paper outlines some preliminary research that assesses the potential of eliminating illegal Spam whilst at the same time allowing companies to use e-mail as a marketing tool, based on cooperation between the Law and the IT Sciences.

Keywords: Internet Service Provider, ISP, Regulation, Legislation, Spam, Junk Mail

1 Introduction

The phenomenal growth of the global Internet and e-mail as the new means of communication enables us to share data more easily and efficiently than ever before. Email is already an efficient method of soliciting customers and selling products. It has proved to be successful not only in the business arena, but also for the millions of families and home users.[1] As small consumers obtain email addresses, the efficiency of using email as a marketing tool will grow. However, this new technology brings with it a new set of problems. While this may good news for advertisers, it is a problem for Consumers, Corporations and Internet Service Providers. *Unsolicited Commercial email*, which is commonly called *'Spam'*, impinges on the privacy of individual Internet users. It can also cost users in turn of the time spent reading and deleting the messages, as well as in a traditional economic sense where users pay time-based connection fees. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of Internet etiquette.

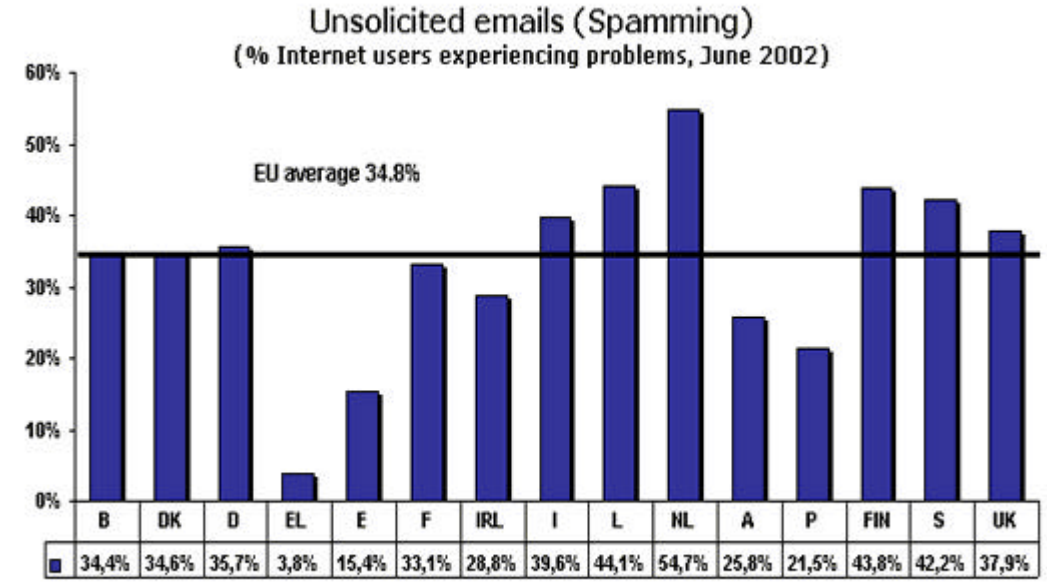
This paper begins by looking at the problems caused by spam, and in this way identifies groups who are affected in different ways (the stakeholders). The roles

[1] According to [1] the number of email boxes world-wide is expected to more than double by 2005. The same IDC report estimates that email messages sent per year will increase from 9.7 billion in 2000 to 35 billion in 2005.
According to [2] email messaging has increased at a compound annual growth rate (CAGR) of 40% since 1981.

played by the stakeholders are discussed, including the measures they are adopting to address the problem. A summary of the different approaches (including strengths and weaknesses) will then be given, and some recommendations made.

2 The different sides of the problem

Internet subscribers world-wide are unwittingly paying an estimated €10 billion a year in connection costs just to receive "junk" e-mails, according to a study undertaken for the European Commission [3]. The study, which provides detailed information on the junk mail phenomenon in both the US and the European Union, forms part of the Commission's ongoing efforts to ensure that the development of the internet and e-commerce does not undermine Europe's rules on Internet privacy and data protection.



Source: European Commission (Eurobarometer June 2002)

The solution to the spam problem is not one easily solved. Senders of spam routinely investigate new and innovative ways to avoid having their emails blocked. Blocking spam by using technology can be difficult because what constitutes spam in one organisation is often a legitimate message to another.

The problems with spam are that firstly consumers have to spend on-line time downloading and reading the spam. As most consumers bear the costs of access they are in effect funding the reception of something they did not want in the first place.[2]

---

[2] "Spamming is the scourge of electronic-mail and newsgroups on the Internet. Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization." by Vint Cerf, Senior Vice President, MCI and acknowledged "Father of the Internet".

Secondly, Spam burdens ISPs who bear much more of the cost of providing the infrastructure than the sender does and frustrates their customers who have to suffer poorer performance levels. Several systems have collapsed due to the sheer bulk of spam. Moreover it creates support overheads for ISPs who must deal with spam complaints from their customers.

Lost productivity is another negative effect of spam. The cumulative costs add up quickly when email users spend a few minutes a day dealing with and disposing of spam. Organisations need to examine what percentage of their labour costs are lost because employees are shifting through junk email, not to mention the diversion of attention of data centre and Informations Systems management staff. There are other productivity drains as well: on a legal front, there have been many instances of lawsuits as a result of pornographic and other messages circulated via email in the workplace.

Spam also poses a threat to consumer confidence in e-commerce. A significant proportion of spam contains fictitious information about the sender, misleading subject lines and extravagant earnings or performance claims in respect of chain letters, pyramid schemes, advertisements for pornographic web sites, offers of software for collecting e-mail addresses, "quack" products and remedies, and illegal software.

Finally, one of the biggest problems of Unsolicited Commercial Communication is that more than 98% [4] of computer viruses now arrive via spam**,** cleverly camouflaged with introductory messages like 'I love you' or tempting picture attachments of Britney Spears, Madonna or Anna Kournikova. The Melissa virus was significant in that it was the first major example of spam effectively "hijacking" the user's computer.

3 The Stakeholders

3.1 Internet Service Providers (ISPs)

No matter how the Internet may be transformed and in what ways its transformation may impact the user, as long as they wish to use it they will need someone to provide them with access services. Internet Service Providers have become a critical component of the commercial Internet providing customers Internet access, web hosting services, e-commerce technologies, and email access. The core player that is most capable of tackling the problem of Spam, is the ISP. According to the Electronic Commerce (EC Directive) Regulations 2002, ISPs are 'mere conduits' – that is, they merely provide the vehicle for the communications to take place. As a result they are not considered liable for the content of information they transmit through their networks. Clearly, if they are not legally liable they have no official responsibility for the content that is transmitted. In general then, they are not expected to monitor every single email. However, in some circumstances ISPs do accept liability as a result of other legal demands:

Contractual liability. If the ISP guarantees a spam-free email service then they are liable towards their customers in case the customers should receive unsolicited

emails. Several ISPs offer newsgroup services to users. There are legal cases where ISPs were sued because they were responsible for filtering the content of the groups. If the ISP claims to the public and its members that it controls the content of its computer bulletin boards then e-mails should be checked before they are published.

Liability after notice. If an individual has identified a defamatory statement, and has forwarded it to the ISP, then the ISP is required to take action – that is, they must remove the statement from the mailing list/newsgroup and send a warning message to the sender of the statement. The provider would have a 'hot line' or 'emergency e-mail address' for members to report defamatory statements so that they can be removed quickly if necessary and corrections made (a copy of the allegedly defamatory material should be attached for quick consideration).

Liability deriving from Article 7 Data Protection Act (UK)

> *Article 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

Since electronic mail addresses, other than business addresses, are deemed to be personal information, the above legislation imposes some restrictions and obligations on how these addresses and other personal information are collected, used and disclosed by ISPs in the course of their commercial activity. The law also creates an obligation for these firms and others who store electronic mail addresses to provide appropriate security for this personal information. Firms buying, selling, leasing or bartering electronic mailing lists (which are the basis for bulk unsolicited electronic mail), will be subject to the provisions of the legislation, providing these transactions take place over provincial and national borders.

Unauthorised forms of messaging. Spam and viruses are affiliated. More than 98% of computer viruses arrive via spam, cleverly camouflaged with introductory messages or tempting picture attachments. If the ISP provides virus protection for which customers have to pay an extra fee, and despite the protection computers get infected, then the ISP is liable under the Computer Misuse Act of 1990. A virus is a malicious programming code that can take the form of a Trojan horse. Such viruses can take control of the recipient's computer and cause damage, such as ruining the file allocation table on the hard disk.

Non-Effective ISP Anti-Spam Techniques that raise liability. ISPs could be liable in the event that providing anti-spam software may cause loss to a communicating user or third party. ISPs deal with spam in a variety of ways, including automatic filtering technologies, as well as customer-controlled filtering services. In January 2003 AT&T WorldNet unsuccessfully tried to use a "reverse DNS lookup" to block spam. ISP servers were programmed to check the incoming e-mail's originating address to a valid domain name or Web address by looking it up in a DNS database; if the address was not there, the message was blocked. This approach failed in that too many legitimate emails were blocked. There have been several cases where ISPs

incorrectly blocked legitimate personal communication, mis-identifying them as unwanted email. Legitimate messages were wrongly tagged as junk mail with the result that half went to junk-mail folders and half were never delivered. These actions raise liability and individuals/companies could claim compensation.

3.2 Government – Legislation

Governments are producing legislation to secure the E-Commerce environment. The term legislation includes national laws such as the Canadian Code of Practice for Consumer Protection in E-Commerce, the United States Act of 2000 for Unsolicited Commercial Electronic (UCE) Mail, or other legislative bodies such as the European Union, EU Directive 2002/58. In this paper we have decided to focus on a summary of the EU Legislation.[3]

a) EU Legislation

The British Government is being urged to consider tougher action on spam. Labour MP Derek Wyatt, chairman of the parliamentary Internet committee, has called on the government to bring Internet service providers under stricter control in an effort to stem the flow of unsolicited pornographic emails. In July 2002 the European Parliament and the Council voted[4] to ban Spam. That means that people will have to "opt in" or ask to receive commercial email. The Directive that was voted to govern spam emails is likely to do little to stem the flow of emails promoting 'get rich quick schemes', pornography and chain letters. Many people are sceptical about the effectiveness of this legislation since much of the spam originates from outside the EU. Two months after the July vote messaging firm Nexor warned that pornographic emails "are on the rise and growing in number by 20 per cent a year"[5].

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[6] (Directive on privacy and electronic communications)

> *(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages … it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them.*

---

[3] This stage of the research compares through evaluation some leading legal cases, the US, the Canadian and European law with respect to ISP responsibility. However, we do not have the space in this paper to effectively provide the comparisons made, and have therefore decided, bearing in mind the European location of the Summer School, to give a summary of the EU Legislation.

[4] Directive 2002/58/EC (12th of July 2002)

[5] http://www.theregister.co.uk/content/6/26771.html

[6] *Official Journal L 201 , 31/07/2002 P. 0037 - 0047*

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC.
(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.
(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments

A summary of the changes:

i) From “opt-out” to “opt-in” (i.e. prior consent)
ii) Except where there is an existing customer relationship (the supplier in this case may use the customer details for the purpose of direct marketing in relation to its own similar goods or services. However, the customer must be clearly and distinctively given the opportunity to object free of charge and in an easy manner to the use of the email address when collected and on the occasion of each message in case the customer has not initially refused such use. This exception leaves open to interpretation whether goods or services advertised are similar to those previously purchased. Moreover it seems from the wording that the exception only applies where there has been an actual sale rather than for example an enquiry. It also appears that only the party that obtained the details can use them: so, for example, a manufacturer could not email its customers where the email address was obtained by a retailer.
iii) Prohibits direct marketing emails disguising or concealing the identity of the sender, or without a valid return address.

Discussion

The proposed provision does not distinguish between 'spam' email, which is bulk, untargeted emails, and direct marketing, where targeted lists are used to develop a specific relationship with customers. Presently most spam originates from outside the EU. European restriction would have little practical effect, however it would put European companies engaged in legitimate direct marketing at a disadvantage, as they are not able to use an effective and increasingly important form of marketing to compete with international counterparts. To impose an opt-in mechanism would require the consumer to request, or consent to receiving, marketing information before it can be sent. The purpose of this is to ensure the consumer is not inundated with information about products and services in which they have no interest. However, this approach has two disadvantages for the consumer: Where a consumer is interested in a specific product or service the consumer will have to request information from relevant companies. Although there will be an awareness of the larger companies, the consumer is unlikely to know about many of many small and medium size companies

who offer similar products/services at competitive prices. This results in a reduction of market competition and a reduction in consumer choice. Consumers may not receive information about new products on the market, which may be of an advantage to them. Direct marketing allows consumers to be informed of new products and services. Without this awareness, consumers will be unable to request marketing information. It is surely for the consumer to decide what communications they receive and to be selective in these choices. An opt-in scheme makes the general decision on behalf of consumers that they will not receive certain communications. This restricts freedom of choice.

Strict legal requirements reduce the impetus for business to develop effective software solutions. The most obvious way to reduce email 'spam' is to develop effective software solutions. This would allow a regulated direct marketing industry to continue but protect the consumer against receiving 'spam' emails. By imposing strict legal requirements the impetus for business to develop effective software solutions is reduced. What is more we have not yet seen any email contain a statement that it is a 'commercial email' or 'unsolicited commercial email' as required by the Electronic Commerce (EC Directive) Regulations 2002 which came into force on 21 August 2002 (SI no 2013). Under those Regulations, an Internet Service Provider must ensure any commercial communication provided by him and which constitutes or forms pan of an 'information society service' must be clearly identifiable as a commercial communication and must clearly identify the person on whose behalf the commercial communication is made.

The Regulations do not prescribe how to meet the requirement for information about commercial communications to be clearly identifiable. The Department of Trade and Industry (DTI) Guidance says this could be either through a header before the communication is opened or in the body of the communication itself. However, the fact that a commercial communication comes from a business may not of itself be enough. The email will need to contain language such as 'this is a commercial communication from Xyz.com Limited.' Furthermore, a service provider must ensure an unsolicited commercial communication sent by him by electronic mail (spam) is clearly and unambiguously identifiable as such as soon as it is received. This is presumably intended to allow the recipient the opportunity to delete the email without opening it or before downloading it perhaps by using some filtering software. Again the Regulations do not prescribe how the requirement for unsolicited commercial communications sent by email to be clearly and unambiguously identifiable should be met.

3.3 Customers – Individuals

Provision of Internet access by ISP's is a highly competitive environment. Customers are the ones that will form the ISP's services. If customers are not satisfied with the quality of services they will change their ISP. The pressure towards better online services, including spam free email communication, will force ISPs to develop anti-spamming software applications and enforce constructive email policies. .

Internet users are empowered by the choice of browsers and other navigation tools. However, consumer awareness is an issue that needs addressing. Some services and programs contain as a "default" a feature giving user consent to receive product or service information. – in other words an "opt-out" system. Consumers should also be

aware that Internet newsgroups, because they are open discussion areas, are frequently used to collect electronic addresses. Collecting these addresses provides an added benefit to marketeers in that user interests are clearly identified.

3.4 Corporations – Enterprises

Enterprises play a double role in the Spam case. On the one hand they do not want to receive any unsolicited email communication from third parties, and on the other, most of them do wish to use email as a marketing tool. Companies can take steps to avoid spam, for example the development of an e-Policy that clearly details how spam is handled. Guidelines about subscribing to email newsletters and web-site that require an email address are critical. E-Policies should also specify how employees handle unsolicited email, especially if the email has offensive or illegal content. In addition, the e-Policy should detail how employees can use email for personal use. Ensuring that employees understand and acknowledge e-Policies is necessary for successful implementation, therefore a training programme or other awareness-raising initiatives may be required. Some written acknowledgement of the policy by the employees is worthwhile as a record of their understanding and willingness to comply. A well-structured email policy can assist organisations in establishing effective e-policies, educating their employees and enforcing e-policies using technology.

3.5 Marketing Associations

Associations of Direct Marketers are also trying to control their members' behaviour online. However, even effective self-regulation by such bodies is ineffective in the junk-mail context insofar that many spammers are not members of any such organisations. The Canadian Marketing Association (CMA) has established for its members a code and guidelines dealing with Internet use for the distribution of promotional materials. Under this code, consumers who are solicited must be given the opportunity of "opting-out" of any further communication from the marketer. A marketer who fails to live up to the CMA code is expelled from the Association.

Another Marketing Association is the Direct Marketing Association (DMA) which is the core trade organisation for all companies involved in direct marketing in the UK and is a member of the International Federation of Direct Marketing Associations and the Federation of European Marketing Associations. The Direct Marketing Association has launched an Email Preference Service with a special Web site (www.e-MPS.org) where consumers and businesses can register their e-mail addresses to opt out on receiving unsolicited e-mail. As part of the "Privacy Promise to American Consumers," which went into effect in July 1999, all DMA members are required to use e-MPS.

4 Current approaches to blocking

Having identified the different stakeholders within the unsolicited commercial email context, we now consider some current methods and techniques that are used in an attempt to alleviate the problem.

4.1 Real-Time Blocking Lists

One of the solutions is to use lists of known spammers, and discard messages originating from those addresses or domains. An example is *MAPS Realtime Blackhole List (RBL)* [5], a free service run by the *Mail Abuse Prevention System*, a non-profit organization dedicated to making the Internet as spam-free as possible. The RBL is a global clearinghouse of information about systems where spam originates and systems that provide support services to spammers. The idea behind the RBL is that a subscriber's e-mail server will consult the MAPS database as each piece of mail is received, and check the sender against the "blackhole list." If the message is coming from a site on the list, it can be discarded, or at least marked as probable spam, before it hits the user's mailbox. Use of a block list can give rise to only one response – to block reception. This technique cannot differentiate between individual emails; all email from the named source will be blocked. However, for some sources of 'dark spam' e.g. known pornographic spammers, blocking is typically the best approach. The problem with the "black list" approach to spam control is that the originating address of a message can be spoofed much more easily than the address of a Web page. Spammers can simply make e-mails look like they are originating from innocuous addresses, or they can continually change the addresses that their messages seem to originate from.

4.2 Content Filtering Technologies

In order to deal with the problem of filtering incoming spam based on originating addresses and to scan inbound and outbound e-mail for confidential information, some sort of keyword examination of the message content is needed. But who can decide what words are offensive? Elron has partnered with the publishers of the Oxford English Dictionary (OED), which is widely recognised as the definitive guide to the English language, to develop a list of offensive terms. The dictionary files can be viewed and modified by systems administrators to customise the product to meet the organisation's needs. Other systems include Mailsweeper that includes amongst other services: keyword filtering of incoming and outgoing messages and protection against viruses in incoming and outgoing messages. However, such systems have not yet overcome the problem of "false/positive" hits (i.e. rejecting a legitimate email based on wrong interpretation of keywords).

Other technical solutions include "bouncing back" suspect emails, and the "honeypot" approach whereby specific email accounts are set up to receive any mail which is then interrogated (a similar is used to detect viruses).

The methods and approaches described above are intended to simply indicate some of the ways used to address the problem of Spam. A full study of these methods would require several papers, at least, and is beyond the scope of this paper. The purpose of this paper is to give an overview of the extent of the problem and some of the solutions currently being provided.

5 Summary and Conclusions

This paper has introduced the problems created by unsolicited commercial communications, and has briefly discussed the legislative measures (of the EU) currently in operation aimed at addressing some of these problems. Whilst these measures are deemed beneficial in that they recognise there is a problem, we have noted some weaknesses.

The effectiveness of the EU Directive is reduced since most spam originates from outside the EU. When a consumer is interested in a specific product or service the consumer will have to request information from relevant companies. Although consumers are likely to know about the larger companies, many of the small companies will be at a marketing disadvantage – i.e. the consumer is unlikely to be aware of the many small and medium size companies offering similar products or services at competitive prices. This results not only in a reduction of market competition but also in a reduction of consumer choice. Strict legal requirements reduce the impetus for business to develop effective software solutions ("if the law is dealing with it, there is no market for us…"). Finally, the Directive does not prescribe how to meet the requirement that information regarding commercial communications should be clearly identifiable. It is very rare that we see any email with a statement that it is a 'commercial email' or 'unsolicited commercial email' in the subject header, as required by the Electronic Commerce Directive.

Technical measures (software applications) can also go someway to address the problem - but they too raise other issues. Using the 'black list' approach to control spam is not effective since the originating address of a message can be falsified very easily. Spammers can simply make e-mails look like they are originating from innocuous addresses, or they can continually change the addresses that their messages seem to originate from. Using Content Filtering Technologies in order to deal with the problem of spam raises the question about who should decide what words are offensive as well as whether inbound and outbound e-mail confidential information is read from unauthorised parties during the filtering process.

Finally there were several cases where ISPs incorrectly blocked legitimate personal communication as unwanted email. Legitimate messages were wrongly tagged as junk mail, half went to junk-mail folders and half was never delivered.

Bearing in mind all of the above, we believe a co-operative approach is needed, utilised by Internet Service Providers as the primary gatekeepers between senders and recipients. Further research will continue in this direction.

References

1 International Data Corporation (IDC) September 2000. http://www.idcresearch.com/
2 GartnerGroup, October 2001. http://www4.gartner.com/Init
3 EU report: http://europa.eu.int/comm/internal_market
4 *Mailwasher* Software Report. Web-user magazine, June 2001.
5 *MAPS Realtime Blackhole List* http://www.mail-abuse.org