Journal of Information, Law and Technology

Spam Law for the Internet

W K Khong
Cyberlaw Centre, Faculty of Management
Multimedia University, 63100 Cyberjaya, Malaysia

wkkhong@mmu.edu.my

This is a **refereed** article published on: 7 November 2001

Citation: Khong W K, 'Spam Law for the Internet', 2001 (3) *The Journal of Information, Law and Technology (JILT)*.
<http://elj.warwick.ac.uk/jilt/01-3/khong.html>

Abstract

This paper briefly surveys the movement to regulate spam or unsolicited commercial emails on the Internet. It discusses the history of spam, definition of spam, and identifies parties fighting spam. Also, it examines legislative efforts in the European Union and the United States to regulate spam and the various schemes and mechanisms employed.

Keywords: Spam, Unsolicited Commercial Email, Unsolicited Bulk Email

1. Introduction - A Brief History of Spam

Spam is a trade mark for a canned meat product from Hormel Foods. In Internet lingo, 'spam' refers to the mass mailing of unsolicited advertisement through electronic means.

The Net Abuse FAQ (Southwick and Falk, 1998) provides a fairly detailed description of the origin of this word. The word 'spam' is commonly ascribed to a skit performed on the British television show Month Python's Flying Circus, in which the word 'spam' is repeated to the point of absurdity in a restaurant menu (*CompuServe Inc. v. Cyber Promotions, Inc. and Sanford Wallace,* 1997). Its usage on the Internet is rumoured to have originated from the MUD/MUSH community where one of the users assigned a keyboard macro to the line: 'SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM' and proceeded to send it to the MUD once every couple of second (Southwick and Falk, 1998). This incident apparently ingrained in the memory of the MUD users and the act was known as 'spamming'.

Spam therefore is the multiple posting of the same message, and spamming is the act thereof. Spam generally appears in two places: emails and newsgroups. Although of late, spam also appears in the form of wireless messages (Balista, 2000). An email spam arise when a message is sent to multiple recipients, particularly for unsolicited advertising purposes.

In the beginning, a distinction was made between newsgroups spam and cross-posting. Newsgroups spamming entails sending an identical copy of the message to every newsgroup, while cross-posting referred to sending a single copy of the message, but addressing it to several different newsgroups (Loundy, 1995). Technically speaking, cross-posting to newsgroups is not spam, because only one copy of the same message resides in every news server (Southwick and Falk, 1998). Most news reader programs are intelligent enough to indicate that a cross-posted message has been read in another newsgroup while the same programs will treat spammed messages in newsgroups as separate unread ones.

Because delivery of emails uses a different protocol from that of news, the ways to combat spam on these platforms are also different. It is easier technically to remove spam on newsgroup through the use of 'cancelbot' and other intelligent agents (Southwick and Falk, 1998). On the other hand, because of the nature of the mail transport protocol which does not require authentication, email spam is difficult to control, and hence receives more attention from the courts and legislatures. In this paper, the focus of the discussion

will be on email spam.

2. Who are Against Spam?

Spam is objected by three groups of people: email users, network administrators, and third parties.

Email users object to spam for the reason that they incur unnecessary cost and time when dealing with undesirable emails in their mailboxes. For users who pay for connection time to the Internet, downloading an additional email which is later found to be useless or a nuisance means money wasted. Even if the user gets his Internet connection free or for a flat fee, he still spends time sifting through his emails, separating junk from genuine. Also, if there is too much spam, the mailbox may overflow and prevent legitimate emails from entering. Email users generally categorise this as a cost-shifting exercise. Because the cost of sending bulk emails, minus the cost to the users, is far too low compared to its perceived success rate, spammers and Internet marketer are in favour of legalising spam instead of banning them (Eccles, 1999).

The practice of sending huge amount of emails to the Internet poses a more serious problem to network administrators. In the first place, a deluge of emails to a mail server may severely cripple the network of an email service provider (ESP). According to a report by an Internet security firm, 14% of Internet email is spam or bulk emails (Wareham, 1999). Netcom, an Internet service provider (ISP), reports that spam increases the cost of support by 15% to 20%, administration by 20%, incoming delivery by 10%, disk space by 15%, and overall equipment cost of 10% to 15% (Dern, 1998). In addition, 5% to 30% of the 14 million emails going to American Online daily are spam (Dern, 1998). The effects of these spam on ISPs are network outages and congestions, and the increasing demand for faster and bigger bandwidth to satisfy the same number of users.

Apart from the increased cost of running a network, ESPs have to bear the brunt of users' complaints when the latter receive spam in their mailboxes. Some frustrated customers threaten to close their accounts unless the ESPs do something to reduce the amount of spam. Hence, spam potentially affects the business opportunity of ESPs and forces network administrators to actively filter spam on their servers.

The third damage done by spam to network administrators is the loss of reputation. Many a times, spammers forge false return email addresses belonging to an ESP, and when angry email users return or bounce the spam, they end up at the ESPs' servers. Unsuspecting Internet users will think that it was the ESPs or network administrators who sanctioned the spam. In addition, severe network outage could result when this email fraud is being carried out.

The last group of spam victims are third parties. These normally are the non-recipients of spam, but are also caught in the disputes when their email addresses or domains are maliciously used in the 'From:' or 'Reply-to:' fields of the spam emails. They are affected when bounced emails or angry emails from recipients are sent to them. It is not impossible for a deluge bounced emails to cripple the server of this innocent third parties.

Trade mark law and the common law of nuisance has been used against this kind of activities.

3. Defining Spam

Even though users' objection differs from network administrators', the solution for both appears to be simply ban spam or the bulk sending of emails. Assuming this step is taken, certain questions have to be considered before such a law is made.

First, what is the basis of such a ban? Under tort law, not all nuisances are actionable. For a nuisance to be actionable, it must be done under negligent or subject to strict liability. Emails and the Internet are such new things that the court has yet to decide whether emails can be subject of nuisance law. Consider this: one difference between emails and other objects of nuisance is that emails become annoying when 'there is too much of a good thing'. Since by having an email address implies the willingness to receive emails, it is difficult to conceptualise the turning point when emails become objectionable. One possible exception to this dilemma is when the user gives explicit notice to a sender that he does not wish to receive further emails from him, and failing to heed the notice gives rise to an action under nuisance law.

Some countries such as the United States have constitutional protection for free speech which raises the question of the extent laws can be enacted to ban spam (Carroll, 1996, Byrne, 1998). In the US, the degree of constitutional protection for political speech is different from commercial speech. Commercial speech gets less protection and can be regulated by law provided the law fulfils certain conditions (*Central Hudson Gas and Electric Corporation v. Public Service Commission of New York* 447 [1980] US, 557). For this reason, the movement to have laws regulating spam mainly cover 'unsolicited commercial emails' as against 'bulk emails', although some states do have 'bulk emails' as a definition (see Appendix I).

The difference between 'unsolicited commercial emails' and 'bulk emails' is succinctly described by Coalition Against Unsolicited Bulk Email, Australia [Caube.au] (n.d.1). It is the inability of US legislatures to regulate communication which may potentially conflict with political free speech protection. In countries where this limitation is less apparent, regulating bulk emails makes better sense than confining regulation to commercial emails.

Another issue is the definition of 'commercial'. Different states and countries may have different interpretations. This may give rise to the problem of over-legislate at one hand, and under-legislate at the other. For example, many services nowadays, such as education, require payment of a fee, and equally many or more websites offer free services to its customers and potential customers. The California Assembly Bill 1676 of 1998 describes 'commercial' as:

> 'advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit',

which is rather comprehensive.

There is a third kind of spam known as acquaintance spam. The Coalition Against Unsolicited Bulk Email, Australia [Caube.au] (n.d.1) explains acquaintance spam as:

> 'spam that is sent to you by somebody you have dealt with previously'.

Acquaintance spam may be problematic in legislating for two reasons. Firstly, often spam from acquaintances is sent in good faith and under the impression that the emails are useful or of interest to the recipients, therefore are more targeted than many of the commercial spam. Secondly, because of prior dealings or contact, the recipient might have implicitly or explicitly consented to the spam. Nevertheless acquaintance spam is still spam, and will take up the network bandwidth, and network administrators will still complain if the load is too much. An extension to acquaintance spam is referral spam - a spam sent by a website through a referral by an acquaintance. Many websites that provide incentives to their users for successful referrals have strict policies against referral spam. This means the users are encouraged to submit referrals, but are prohibited from flooding the system with every email addresses they can find.

The first problem in regulating spam is to define spam. As discussed, this is not a simple problem. Different interpretations have different implications. The utopian definition of spam will net all email communications which are of no benefit to the recipient, from the recipient's point of view, and exclude all those which are beneficial from the same recipient's point of view.

4. The Fight Against Spam

In the early days of the Internet, social behaviour on the Internet was governed by a form of custom, affectionately known as 'netiquette' (Hambridge, 1995). The source of this 'netiquette' or network etiquette is mostly from network administrators' acceptable use policies (Mueller and Pnitz, n.d.). These acceptable use policies serve as agreements between the network administrators and their users on what are and are not acceptable practises when using the Internet. The policies in turn are influenced by the technical limitations of the Internet protocols, which make the Internet function effectively (Hambridge and Lunde, 1999).

With the passing of time, these acceptable usage policies became a custom of the Internet. Network administrators formed a consensus and followed standards. Internet users were presumed to have consented to these netiquettes upon going onto the Net. Any apparent breach was to arouse the ire of other users. Sanctions of various kinds, from reprimands to denials of access, were imposed on offending parties. Sometimes, the network administrator for these offending parties was also rebuked for his inability to solicit proper behaviour from his users. This vigilante or frontier justice (Loundy, 1995) has the effect of compelling new users to take note of the existing netiquette. Commentators suggest that this netiquette has the weight of customary law (Carroll, 1996).

When the Internet was transformed from an academic and research network into a

commercial concern (Zakon, 2001), the scene changed. More non-technical users started to use the Internet blissfully ignorant of the netiquettes. At the same time, commercialisation and advertisements started to appear as part of Internet services and Internet users became more open to commercial content. From then on, commercial spammers began to operate.

One of the first and most notorious spam was inflicted by the US attorney couple Lawrence Canter and Martha Siegel. One day in 1993, they sent out identical 'green card' advertisements to every newsgroup they could locate. They received many prospective leads, but they also found themselves at the receiving end of more angered responses. Some users retaliated by relaying multiple emails to them, causing massive overloading of their mailbox and their network provider's server. Other irate hackers tried to knock down the server by hacking it. One ingenious hacker created a 'cancelbot' to automatically wipe out every copy of the offensive message in the newsgroups.

The Canter and Siegel episode demonstrates clearly that there was some kind of rule in force. There was no court, no arbiter, and no prosecutor. Instead, users took the 'law' into their own hands. Collectively, the sanction imposed could be enormous. This is an evidence of 'mob law' or 'vigilante regulation'.

In time, spammers became wiser. They forged email headers, used unsuspecting public email relay servers, and provided false return addresses. This caused further difficulties to the Internet community, particularly the network administrators. There are many instances where servers using the forged domains were forced to the point of shut down, swamped by bounce emails and unintentional returning hate mails.

Since the first spam, network administrators and Internet users have been devising various technical methods to overcome the problem of spamming. Some include filtering mails going to the email accounts, blocking spam emails from an entire server, blocking Usenet newsgroup spam for an enter server, and blocking IP connectivity from spam sites.

One email service provider tries to bill spammers for the resources they used (R&D Associates, 1998). Their argument is that it is for the:

> 'time required in training [their clients] and cleaning [the] servers, and the space that was used in storing [the spammers'] documents.'

However, so far, they were still far from being successful in their claim.

On the legal side, some email service providers (ESPs) have taken spammers to court based on a few causes of action. From the ESP's point of view, sending unsolicited commercial emails to the ESP's server after repeated request and warning to stop doing so is a trespass to property (*CompuServe Inc. v. Cyber Promotions, Inc. and Sanford Wallace* 962 (1997) F. Supp 1015). This argument has been upheld in the court. Others reasons for action includes the spammers breaching the agreement with their email service providers for sending spam. Also, their spams cause Internet users' retaliation,

which shut down the ESP's server. Further, the forged false headers and return addresses cause innocent businesses network outage and loss of reputation. Action under trade mark infringement and false trade description may also be possible. Spamming is considered an unacceptable activity by the U.S. courts, and the courts have allowed injunctions against spammers to send unsolicited commercial emails to specific sites. More recently, a Canadian court has recognised spamming as against netiquette, which further strengthens ESP's position against spammers (*1267623 Ontario, Inc. v. Nexx Online Inc.* [1999] O. J. 2246, <http://legal.web.aol.com/decisions/dljunk/nexxorder.html>).

5. Legislating Spam

Many countries have passed or are planning to pass law to regulate spam. For example, some states in the US have enacted bills to that effect. In the European Union, the European council and parliament have made several directives pertinent to spam.

5.1 European Union

The study by Gauthronet and Drouard (2001) for the European Commission identified four directives which are relevant in regulating spam.

- The Data Protection Directive (European Parliament and Council; 1995);
- The Telecommunications Privacy Directive (European Parliament and Council, 1998a);
- The Distance Selling Directive (European Parliament and Council, 1998b); and
- The Electronic Commerce Directive (European Parliament and Council; 2000).

5.1.1 Data Protection Directive

The Data Protection Directive is the European form of privacy protection for personal data. It establishes a property right in personal data, by which a data subject may exercise certain exclusionary rights against the collection and processing of data against him. According to the European Commission's study (Gauthronet and Drouard, 2001), email addresses are a form of personal data as defined in Article 2(a) of the Data Protection Directive. The test is that the data is capable of relating to an identified or identifiable human data subject.

Several safeguards are provided for the data subjects when data is processed or collected (Data Protection Directive, Art. 7). Before data such as an email address is collected, the unambiguous consent of the data subjects needs to be sought. Where the data is not obtained from the data subject directly, the subjects must be informed of the collection at the time of recording. When disclosure to a third party is envisaged, the data subjects

must be informed no later than when the data is first disclosed (Data Protection Directive, Art. 11). The idea of 'processing' under the Data Protection Directive is extremely broad, and covers:

> 'collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction', of the personal data (Data Protection Directive, Art. 2(b)).

Most importantly, in respect of direct marking, a data subject is granted the right:

> 'to object, on request and free of charge, to the processing of personal data relating to him' (Data Protection Directive, Art. 14(b)).

That means, he can prohibit his email address from being collected and subsequently used for the purpose of spamming.

5.1.2 Telecommunications Privacy Directive

The Telecommunications Privacy Directive of 1997 provides that:

> 'the use of *automated calling systems without human intervention (automatic calling machine)* or facsimile machines (fax) for the purpose of direct marketing may only be allowed in respect of subscribers who have given their prior consent' (emphasis mine) (Art. 12(1)).

Further,

> 'free of charge, unsolicited calls for purposes of direct marketing, by means other than [automatic calling machine or fax] are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation.'

Austria, Denmark, Finland, and Italy have thus enacted national laws according to this Art. 12(2) to include spam or unsolicited commercial emails by including email services as a form of 'automatic calling machines'. The basic rationale of the Telecommunications Privacy Directive is very much similar to the Data Protection Directive, i.e. to protect the data privacy of the telecommunications users.

5.1.3 Distance Selling Directive

The Distance Selling Directive of 1997 repeats *ad verbatim* the position taken in the Telecommunications Privacy Directive (Art. 10). Interestingly, although the language used is exactly the same with that of the Telecommunications Privacy Directive, the rationale is different. The Distance Selling Directive is mainly a form of consumer protection law in the context of distance selling.

5.1.4 Electronic Commerce Directive

6 May 1999 marks a failed attempt to explicitly ban unsolicited commercial emails in the European Parliament, when 266 members voted against a ban while 137 voted in favour of it (EuroCauce, 1999). On 8 June 2000, the European Parliament and Council adopted an Electronic Commerce Directive which incorporated the labelling and opt-out mechanisms. Member states have up to 17 January 2002 to implement this directive.

This Electronic Commerce Directive of 2000 takes a slightly different approach as to spam. It allows member states to enact law permitting unsolicited commercial emails, provided that the sender is clearly and unambiguously identifiable (Art. 7(1)). It also requires spammers to regularly consult and respect of opt-out register by service providers (Art. 7(2)).

This directive is ambiguous in certain respects and subject to criticisms (Gauthronet and Drouard, 2001). Although, the sender's identity has to be clearly stated, it does not necessarily mean that the spammer is obliged to act upon requests for removal from a mailing list. Also, the identification process does not necessarily mean that the request for removal process is costless. A spammer which provides a phone number for the request for removal process may charge a high free for such removal through 600 numbers. Further more, the directive does not state that the opt-out register must be consulted every time before a spamming exercise, but merely regularly. Finally, the directive does not indicate how an opt-out register is to be constructed, i.e. whether a single register for the whole European Union, or multiple industry registers which reduces the incentive of spammers to check every register and email users to register in the same. There could also be high evidential cost as to whether a spammer has 'regularly' checked an opt-out register.

It is clear that the position of the Electronic Commerce Directive is heavily influenced by the direct marketing industry. Instead of conferring a right not to be spammed on email users, it indirectly sanctioned spam. From a theoretical point of view, we may say that the Electronic Commerce Directive is in support of the freedom of the competitive market.

5.1.5 European National Laws

At the time of writing, Austria, Denmark, Finland, Germany and Italy have laws to regulate commercial or unsolicited emails (Caube.au; n.d.2). Austrian law requires the prior revocable consent of the recipient <http://www.euro.cauce.org/en/countries/c_at.html>. In Denmark, unsolicited emails are prohibited <http://www.euro.cauce.org/en/countries/c_dk.html>. In Finland, sending of unsolicited commercial emails to private person and newsgroups is unlawful <http://www.euro.cauce.org/en/countries/c_fi.html>. In Germany prior consent is required for all contacts through development of case law on unfair competition <http://www.euro.cauce.org/en/countries/c_de.html>, but in Italy, this is only confined to emails for advertising purposes <http://www.euro.cauce.org/en/countries/c_it.html>.

5.2 United States of America

Some efforts have been made by the federal and state legislatures of the US in regulating spam. As in the usual case, pressure groups play an important role in laws-making in the United States. The most vocal group in promoting a ban against spam is the Coalition Against Unsolicited Commercial Email (CAUCE) <http://www.cauce.org/>, which has counterparts in other countries, i.e. European Coalition Against Unsolicited Commercial Email (EuroCauce) <http://www.euro.cauce.org/en/>, Coalition Against Unsolicited Bulk Email, Australia <http://www.caube.org.au/>, and Coalition Against Unsolicited Commercial Email, India <http://www.india.cauce.org/>. On the other hand, the Direct Marketing Association <http://www.the-dma.org/> serves the interest of the mailing list industry.

5.2.1 Federal Law

Law-making at the federal level has not yet been successful. Various bills were presented at the Senate and House of Representatives by the pro and anti-spam proponents. However, none has passed into law.

In the 106th Congress for the term of 1999 to 2000, a total of ten bills were presented at the House of Representative and the Senate (Sorkin, n.d.2). In the present 107th Congress, five bills have so far been proposed.

One novel approach to tackling spam at the US federal level is to modify the language of Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227. The Telephone Consumer Protection Act prohibits, *inter alia:*

> 'the use of any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine'.

Through the Act's overbroad definition of a 'telephone facsimile machine', it is possible to cover unsolicited advertisement emails (Sorkin, 1997).

In 1997, CAUCE proposed an amendment to the Telephone Consumer Protection Act to explicitly cover unsolicited commercial emails. This proposed amendment was taken up by Repulican representative in the House of Representatives, Christopher Smith. On 21 March 1997, he presented his Netizens Protection Act of 1997 to the House. With the amendment, not only is spam outlawed, Internet users who are spammed get a private right of action to sue the spammer US$500 for each message. If the court believes that the spammer wilfully or knowingly violated the law, the claims are tripled. However this amendment died in the 105th Congress.

Another notable proposal is the Unsolicited Electronic Mail Act of 1999 (H.R. 3113) in the 106th Congress. This bill seeked to incorporate the best parts of earlier bills and provisions in the state laws. These include the requirement of a valid return email address, and provisions which:

- force spammers to honour opt-out requests;
- outlaw forged headers;
- empower ESPs to bring spammers to court for violating access policies;
- allow ESPs to collect payment for sending spam to their users;
- allow ESPs to implement spam filters;
- allow individuals and corporations to use spammers in civil court;
- authorise the Federal Trade Commission to pursue violation of law; and finally,
- provide for an exception where the sender and the recipient have an existing business relationship but retains the right to rescind permission by the recipient.

By far, it is the most comprehensive of all, although it still falls short of what most anti-spam advocates want - the banning all but opt-in schemes.

Although this bill has gone through various amendments in the House of Representatives, two of its reincarnations are still alive in the 107th Congress.

5.2.2 State Laws

At the time of writing, 18 states in the US have enacted laws relating to spams (Geller, 1999, Sorkin, n.d.1). They are: California; Connecticut; Delaware; Idaho; Illinois; Iowa; Louisiana; Missouri; Nevada; North Carolina; Oklahoma; Pennsylvania; Rhode Island; Tennessee; Virginia; Washington; and West Virginia. State legislation started with Nevada (1997). This was followed by Washington, California and Virginia. The laws passed by these four states subsequently became models for the other ten states (Geller, 1999). A summary of the provisions is given by Sorkin (n.d.1).

6. Regulatory Mechanisms

Different regulatory mechanisms were introduced in the state laws passed in the US. These mechanisms vary from allowing the sending of spam, to a limited right to send commercial emails. They include the requirement to have true routing information, valid identification in the email, provision for out-out scheme, identifier in subject line to aid filtering tools, SMTP banner notification, and clean-up damages for affected parties. In most cases, the laws incorporate a mixture of these mechanisms. That aside, anti-spam proponents as represented in the European directives have advocated a revocable opt-in scheme or an outright ban.

A breakdown of these regulatory mechanisms by US state laws is provided in Appendix I. Sorkin (2001) further discusses some of these mechanisms.

6.1 True Routing Information

Advanced spammers use special programs to send spam with spoofed routing information. Spoofing is the introduction of false or inaccurate headers in emails in order to fool servers and users into thinking that the emails came from a certain location. The danger of spoofing is that it may cause harm to an innocent network administrator when his server becomes the target of bounced emails and mail bomb attacks. Realising this, almost all spam laws require that routing information must not be falsified and the identity of the sending party be maintained.

6.1.1 Banning Spoofing Spamware

For the same purpose, software which allows modification or falsification of routing information for the purpose of sending spam is also banned. In some cases, distributing or selling of this kind of software is a criminal offence.

6.2 Valid Email Addresses

Because of flames and mail bombs from angered spam recipients, many spammers do not use valid email addresses and email headers in their spam. However, this causes difficulties for spam recipients to contact the spammers in order to request not to be spammed in the future. Therefore, state laws such as the California Assembly Bill 1676 (1998) requires a 'valid sender operated return e-mail address'.

6.3 Opt-Out Schemes

The requirement of a valid return email address is tied closely to the implementation of opt-out schemes. An opt-out scheme gives a spammer the right to send spam to recipients unless the recipients email or sign up a form to inform the spammer that they do not wish to continue receiving spam from him. This is the mechanism most favoured and championed by the Direct Marketing Association (Eccles, 1999). Two types of opt-out schemes exist: spammer-specific opt-outs and opt-out registers.

6.3.1 Spammer-Specific Opt-Outs

Spammer-specific opt-outs refer to the legal recognition that a spam recipient has the right to withdraw a spammer's right to send spam to his email address in the future. Often, when this right is recognised, the law mandates that the spammer has to provide clear information in his email on how to opt-out, and an email address or toll-free telephone number for this purpose. Spammers who fail to respect this right are liable for damages and possibly criminal prosecution. To provide the spammer time to update his mailing list, sometimes a grace period of five days from the communication of an opt-out

request is given.

6.3.2 Opt-Out Registers

Opt-out registers were first introduced in the direct mail industry as a response for a call to regulate commercial mails (Sovern, 1999). The US based Direct Marketing Association has extended the idea to spam by introducing an e-Mail Preference Service (Direct Marketing Association, n.d.). The e-Map Preference Service works by allowing a spammer to send his list of email addresses to the service and let the service 'clean up' addresses which have been registered. What proponents of opt-out scheme fail to see is that this system can easily be subjected to abused.

The opt-out register is criticised for various reasons. First there is no proof that spammers will honour such an opt-out scheme. In fact, it has been shown that spammers are not members of the traditional direct marketing organisations, which understands the value of self-regulation. Most spam is a one-time spam from advertisers. If every potential advertisers sent one spam each, much time and effort would have to be wasted to opt out. Even if the spam recipient sends an email or filling in a web-based form to opt-out, it will be taken as a sign that the email is valid and alive. The effect is that the email address is more valuable and more spam will ensue. Similarly, a simple computer program may be used to compare the source and output of the e-Mail Preference Service to single out those addresses that have been removed. These addresses would be more valuable because the addresses are alive and valid, and that the recipients have taken an active effort to register themselves with the service. This will also cause more spam to the addresses. Studies have shown that the longer an email account is being used, the more spam it will receive (Riggs, 1999). One reason could be that the addresses are sold to the spammers.

Although the use opt-out register is the one most disfavoured by anti-spam advocates, legislatures are frequently pressured by the direct marketing industry to introduce a compromise. Currently, only the state of Colorado recognises the use of an opt-out register, though not mandating its use.

6.4 Identifiers in Subject Line

6.4.1 Filter Friendly Identifiers

One other control mechanism that has been suggested is to use an email filter. Although this does not at all reduce the amount of spam, it helps recipients filter unwanted emails. To enable this filtering mechanism to work more efficiently, a specific keyword has to be place in the email header. The best place to do so is at the subject line of the emails. The advantage in using this system is that emails may be filtered at the ESP's level before being downloaded into the user's computer.

The California Act for example, requires all unsolicited commercial email to have the words 'ADV:' at the beginning of the subject line, and 'ADV:ADLT' if the spam

contains adult advertisement (Geller, 1999). Since there is only one subject line in each email, to make this system work, all laws implementing the mechanism must use the same keywords. Hence, Colorado's law requires the same implementation as California's.

For this mechanism to work effectively, there must be a standardization of the keywords. Much like content code for movies, either the industry or the international efforts must agree on a content code-like identifiers for spam. On the other hand, like a paradox, once users rely on this mechanism, the effectiveness of spam will decline immediately.

6.4.2 Non-Misleading Subject Lines

A less effective solution is the requirement of non-false or misleading subject lines in spam emails. Although theoretically, this saves spam recipients the trouble of having to read through the body of spam emails to know that they are junk, it is less elegant compared to filter-friendly identifiers. The concept of legitimate unsolicited spam will be meaningless. The state of Washington has a provision requiring non-misleading subject lines.

6.5 ESP Filtering and Blocking

End user filtering however is not effective. As spammers rarely use the same sender's address twice, filtering by identifying the sender is hardly successful. ESP-level filtering may yield a better result. When a spam has been identified, the ESP could scan his server for spam and delete it, saving users the anguish of downloading it.

Blocking, on the other hand, is the refusal of servers to allow relaying of emails coming from certain IP addresses. Blocking is normally done by the email service providers. Collective efforts to maintain a Realtime Blackhole List (RBL) have proved to be effective in blocking spam at its source. A blackhole list is a list of IP addresses which are known to assist or friendly to spammers (Loren, n.d.). Under this system, a email relay server will first check the RBL for the connecting IP address. If the IP address of the sender matches one on the list, then the connection gets dropped before accepting any traffic from the spammer.

Treatment of blocking varies among jurisdictions. Some state statues in the US sanction blocking by the email service provider. However, in a recent case in New Zealand, a high court has issued an injunction against the administrator of a blackhole list, the Open Relay Behavioural Modification System (ORBS), for including a website's IP address in its blackhole list (Foreman, 2001).

6.6 SMTP Banner Notification

This is another technological innovation to control spam. According to CAUCE, legal recognition of a 'no-spam' SMTP banner will pave the way for the enforcement of anti-spam policy based on technology (Cauce, n.d.). The SMTP banner notification allows the network administrator of a mail server to configure its server to send a 'no-spam'

message to any servers requesting permission to send emails. This shortcuts the need for human intervention and notification before sending spam become a trespass. The Californian bill contains a provision recognising the use of SMTP notification service. Similarly, the Can Spam Act (H.R. 2162, 1999) introduced by Rep. Garry Miller of California contains a provision for recognition of SMTP banner notification.

6.7 Revocable Opt-In Scheme

By far, opt-in scheme is the most favoured by anti-spam advocates. Opting-in means that the recipient has actively given prior consent to send commercial emails to him. The advantage of opt-in scheme is that it reduces the number of spam on the Internet, and recipient could not complain since they have given consent. To make an opt-in scheme work, it must be the only mechanism allowed by law. When the recipient no longer wishes to receive the emails, a corresponding opt-out method must be provided by the advertisers. Unlike the US, many European countries have adopted an opt-in scheme as the only lawful way of sending commercial emails.

6.8 Outright Ban

The pristine view that the Internet should be free from all commercial activities has long gone since the National Science Foundation has relinquished its control over the Internet backbone in 1995 (Zakon, 2001). Although some countries such as Denmark and Italy have laws which prevent direct marketing, the general consensus is that an outright ban would be inconceivable to the growth of the Internet. As stated, the more preferred mechanism is to ban unsolicited commercial emails and legalise opt-in solutions.

6.9 Damages

Damages is a good deterrent against spam. Many laws provide statutory damages to individuals and ESPs. These damages vary from US$10 per message in Colorado and Iowa to US$500 in Rhode Island. Besides, there is a cap on the maximum claimable amount of statutory damages. Some states also allow recovery of actual damages to spam recipients and network administrators.

7. Need for International Co-ordination

There is a serious need for international co-ordination to successfully tackle the spam problem. This stems from the fact that many a times, the spammer and recipients are from different states or countries, each subject to a different set of laws. Jurisdiction based on the recipient's location is problematic. That would mean that the spammer would have to profile in detail each email address, and have knowledge of many sets of laws. Also, the domain name of a recipient's email address does not indicate where the recipient actually is. Harmonisation efforts at the federal level in the US, and commission level in the EU are moving in the direction to solve this problem. A long term solution will only appear when the broader jurisdiction question of the Internet is tackled.

8. Conclusion

This paper is a preliminary study of the movement to regulate spam on the Internet. There is still no global consensus as to the proper regulatory mechanism. Further, the issue of transborder spamming activities are yet to be adequately resolved and more studies and discussion have to be conducted. As email addresses are not an indication of the recipients' physical location, it would be technically impossible to prevent a commercial email from reaching a recipient in a country that outlaws spam. Like many of the cyberlaw issues, an agreed global protocol would have achieved many milestones in the fight against spam on the Internet.

Acknowledgement

The Multimedia University for providing financial assistance for conducting this research. Special thanks go to participants in the 15th Annual Conference of the British and Irish Legal Technology Association for their helpful comments.

References

Batista, E (2000), 'A Fight to Ban Cellphone Spam', WiredNews, July 6, <http://www.wired.com/news/business/0,1283,37376,00.html>.

Byrne, J (1998), 'Squeezing Spam Off the Net: Federal Regulation of Unsolicited Commercial E-mail', West Virginia Journal of Law & Technology, 2(1), <http://www.wvjolt.wvu.edu/v2i1/byrne.html>.

Carroll, M W (1996), 'Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations', Berkeley Technology Law Journal, 11(2), <http://www.law.berkeley.edu/journals/btlj/articles/11_2/Carroll/html/reader.html>.

Coalition Against Unsolicited Commercial Email. (n.d.). 'SMTP Banner Notification Proposal', <http://www.cauce.org/proposal/index.shtml>.

Coalition Against Unsolicited Bulk Email, Australia (n.d.1) 'What is Spam?', <http://www.caube.org.au/whatis.htm>.

Coalition Against Unsolicited Bulk Email, Australia (n.d.2) 'National Laws Overseas', <http://www.caube.org.au/natlaws.htm>.

Dern, D P (1998), 'Postage Due on Junk E-Mail: Spam Costs Internet Millions Every Month', InternetWeek, 713, May 4, <http://www.techweb.com/se/directlink.cgi?INW19980504S0003>.

Direct Marketing Association (n.d.) 'e-Mail preference service', <http://www.e-mps.org/en/>.

Eccles, M (1999), 'Opt-Out System is the Right Way to Tackle Spam', Marketing Week,

May 20, at 42.

European Coalition Against Unsolicited Commercial Email (1999) 'Result of Vote on UCE Ban', <http://www.euro.cauce.org/en/vote_result.html>.

Foreman, M (2001), 'Court Forces ORBS to Remove Xtra E-mail From Blacklist', The New Zealand Herald, May 29, <http://www.nzherald.co.nz/storyprint.cfm?storyID=191406>.

Gauthronet, S and Drouard, E (2001), Unsolicited Commercial Communications and Data Protection, (Brussels: Commission of the European Communities, Internal Market Directorate General), Contract no. ETD/99/B5-3000/E/96, <http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spam.htm>.

Geller, T (1999), 'State Law Update', Cauce News 3(4), <http://www.cauce.org/newsletter/v3n4.shtml>.

Hambridge, S (1995), 'Netiquette Guidelines', (IETF RUN Network Working Group, RFC 1855), <http://www.ietf.org/rfc/rfc1855.txt>.

Hambridge, S and Lunde, A (1999), 'Don't Spew: A Set of Guidelines for Mass Unsolicited Mailings and Postings (Spam*)', (IETF RUN Network Working Group, RFC 2635), <http://www.ietf.org/rfc/rfc2635.txt>.

Loren, L P (n.d.), 'Regulating Cyberspace: A Case Study of Spam', <http://www.cyberspacelaw.org/loren/phase3.html>.

Loundy, D (1995), 'Lawyers' Electronic Ads Leave Bad Taste', Chicago Daily Law Bulletin, March 9, at 6, <http://www.Loundy.com/CDLB/Spam.html>.

Mueller, S H and Panitz, A R (n.d.), 'Sample Acceptable Use Policies', <http://spam.abuse.net/spam/aup.html>.

R&D Associates (1998) 'History of a Dispute with a Spammer', <http://www.kclink.com/spam/>.

Riggs, B (1999), 'After a While, It All Looks Like Spam', Information Week, June 7, at 14.

Sorkin, D E (1997), 'Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991' Buffalo Law Review 45, at 1001-1032.

Sorkin, D E (2001), 'Technical and Legal Approaches to Unsolicited Electronic Mail', University of San Francisco Law Review 35, at 325-384, <http://www.spamlaws.com/articles/usf.pdf>.

Sorkin, D E (n.d.1), 'Spam Laws: United States: State laws: Summary',

<http://www.spamlaws.com/state/summary.html>.

Sorkin, D E (n.d.2), 'Spam Laws: United States: Federal Laws: 106th Congress: Summary', <http://www.spamlaws.com/federal/summ106.html>.

Sorkin, D E (n.d.3), 'Spam Laws; United States: Federal Laws: 107th Congress: Summary', <http://www.spamlaws.com/federal/summ107.html>.

Southwick, S and Falk, J D (1998), 'The Net Abuse FAQ', <http://www.cybernothing.org/faqs/net-abuse-faq.html>.

Sovern, J (1999), 'Opting In, Opting Out, or No Options At All: The Fight to Control of Personal Information', Washington Law Review 74, at 1033-1188.

Wareham, E (1999), 'Spam and E-Mail Abuses Costing Millions: Survey', Computing Canada, 25(19), at 1.

Zakon, R H (2001), 'Hobbes' Internet Timeline v5.3', <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>.

Cases

1267612 Ontario, Inc. v. Nexx Online Inc., [1999] O.J. No. 2246 (Court file no. C20546/99), <http://legal.web.aol.com/decisions/dljunk/nexxorder.html>.

CompuServe Inc. v. Cyber Promotions, Inc. and Sanford Wallace, 962 F. Supp. 1015 (S.D. Ohio Feb 3, 1997).

Central Hudson Gas and Electric Corporation v. Public Service Commission of New York, 447 U.S. 557 (1980).

European Directives

European Parliament and Council (1995) 'Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal L. 281, November 23, at 31-50, <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html>.

European Parliament and Council (1998a) 'Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector', Official Journal L. 24, January 30, at 1-8, <http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf>.

European Parliament and Council (1998b) 'Directive 97/7/EC of the European Parliament and the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts', Official Journal L. 144, 4 June 1997, at 10-27, <http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf>.

European Parliament and Council (2000) 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market', Official Journal L. 178, July 17, at 1-16, <http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf>.

Appendix I: Summary of Regulatory Mechanisms in U.S. States' Spam Laws

State	Type	True Routing Information	Prohibits Spoofing Software	Valid Sender/ Return Address	Opt-Out Information	Toll Free Opt-Out Number	Opt-out Register	Identifier in Subject Line	ESP Filtering/Blocking	SMTP Banner Notification	Damages
California	UCE		Yes	Yes	Yes		ADV:	ADV:ADLT	Recognised	ESP: actual damages or $50 per email (max $25,000)	
Colorado	UCE	Yes	Yes		Yes		Recognised				
	ADV:	Yes	$10 per email								
Connecticut	UBE	Yes	Yes								
	$10 per email or $25,000 per day										
Delaware	UBCE	Yes	Yes	Yes	Yes						
	Yes	Recipient: Actual damages, $100 per email, or $1000									
Idaho	UBCE	Yes			Email address						
	Yes										
Illinois	UCE	Yes	Yes	Yes							
	Yes	Actual damages, $10 per email, or $25,000 per day									
Iowa	UBE	Yes		Yes	Yes						
	Yes	ESP: Actual damages, $10 per email, or $25,000 Others: Actual damages, $10 per email, or $500									
Louisiana	UBE	Yes	Yes								
	Yes										
Missouri	UCE			Yes	Email address		Yes				
	Yes	Recipient: Actual damages or $500 ESP: Actual damages or $1000									
Nevada	UCE			Only required in body	Yes						
	Ambiguous	Recipient: Actual damages or $10 per email									
North Carolina	UBCE	Yes									
	Actual damages, $10 per email, or $25,000 per day										
Oklahoma	UBE	Yes	Yes								
	Actual damages, $10 per email, or $25,000 per day										
Pennsylvania	UCE (Explicitly sexual)			Yes	Email address						
	ADV-ADLT										
Rhode Island	UBE	Yes	Yes	Yes	Yes	Yes					
	Yes	Actual damages, $500 per email, or $25,000 per day									
Tennessee	UCE		Yes	Yes	Yes		ADV:	ADV:ADLT	Actual damages, $10 per email, or $5000 per day		
Virginia	UBE	Yes	Yes								
	Yes	Actual damages, $10 per email, or $25,000 per day									
Washington	UCE			Yes				No	misleading subject line	Yes	Recipient: Actual damages or $500 ESP: Actual damages or $1000
West Virginia	UBE		Yes	Yes				No	misleading subject line	Yes	Recipient: Actual damages, minimum $1000, or punitive damages ESP: Actual damages, $10 per email, or $25,000 per day