The regulation of spam

A theoretical and practical analysis

Max Mailliet☐
☐
max@mailliet.lu☐
☐
London School of Economics and ☐
Political Science

Introduction

> ***"Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. ... Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization."***
>
> Vint Cerf, Senior Vice President, MCI
> and acknowledged "Father of the Internet"[1]

There can now be no doubt that a new era of internet usage has come upon us with the rise of spam: the usage of email is becoming more burdensome by the day. The daily "walk" to an email user's[2] inbox has become a trip to an intensely populated horror house where he will be welcomed by an overcrowded mailbox filled with commercial email messages or scams, sent in bulk to millions of users who never solicited them. In everyday language, these are called spam.

The history of commercial spam traditionally starts with the account of the Canter and Siegel "incident"[3]. Ironically, Canter and Siegel were two lawyers offering "green card" services. They found out that by sending the same message containing the advertisement of their services to thousands of Usenet groups, they could reach a very large audience to sell their services to. The reactions to their action were much differentiated: some users did indeed use their services, but others reacted violently by sending infuriated emails to the two lawyers and even took some worse actions[4].

In any case, the overall result was clear: the sending of mass emails[5] for commercial use had just been invented. As a matter of fact, this incident that happened in April 1994 marked the

---

[1] Source : www.cauce.org

[2] I will refer to email users as "recipients"

[3] For a detailed account on how the era of spam came upon us and where the name "spam" comes from, see http://www.templetons.com/brad/spamterm.html

[4] These included the setting up of systems to flood the lawyer's voicemail, death threats, "cancelbots" which are supposed to remove their messages from the Usenet groups and much more, see for instance Leeper and Heeler, *Commercial Speech in Cyberspace: The junk email issue*

[5] Which will later be known as "spamming"

birth of spam. Since then, the level of sent spam is increasing everyday, with spam making up for about 65% of the total amount of emails sent everyday[6].

The spam business model[7]

Spam functions through a business model of its own: bulkiness. The sending of emails to millions of persons is not significantly more expensive than sending an email to one person only. The spammer then relies on the assumption that even if only 1% or less of the targeted people (e.g. one million) take up the offer contained in the email (generally an offer for a supposedly cheap loan or to buy some medicines), he will have sold his products 10.000 times. A tiny profit margin will already render enormous profits, knowing that spam is usually sent to much more than "just" a million addresses. It becomes quickly clear how the spam business model is commercially interesting, a minimal marketing effort resulting in the making of large amounts of money.

Recipient's reactions: self-help

Most users, in response to the large amount of spam they receive every day, try to implement technical solutions to counter the problem, mostly in the form of email filtering applications, commonly known as spam filters. But the technical fight against spam has become more difficult again, with spammers inventing new efficient techniques for overriding spam filters, by using special message formats, thus confusing spam filters which let the message pass through[8].

In any case, there can be no doubt that, at present, spam has become an important part of the internet, not by making a positive contribution, but rather by slowly endangering the survival of the internet as we know it today.

I purport to conduct an analysis of how the spam problem could be tackled with in a legal manner. I will be analysing why a legal framework needs to be built and then I will bring up suggestions on how to build it, bearing in mind the recent efforts in anti-spam laws that have been undertaken in the EU and in the US and critically assessing them. This calls for an

---

[6] This figure is correct as of June 2004 and has been provided by Brightmail, an anti-spam service provider (http://www.brightmail.com). The level of spam has risen from 50% in June 2003, and it seems that its ascension will not be stopped in a near future.

[7] See Lloyd, *Legal Aspects of the Information Society*, p. 272

[8] A new tactic is also to include into the spam a message of the same colour as the background and containing information that will make look the message like a personal message.

analysis in three parts: first, I will have to explain why spam is so bad that it needs to be regulated (part 1). Having done so, I will have to address the question of how to define spam (part 2) and then move on to the issue of how to address the spam problem with legislation (part 3).

I. Why is spam so bad?

The question of whether spam is really that bad that it needs to be regulated has been around for some time now. To argue that their practice is legitimate, spammers have always compared themselves to advertisers. They have continuously argued that spam is no worse than television advertisements, or, for instance, advertisements being shown in or on buses or along roads. However, a point has to be made: television advertisements contribute in financing the service, which means that they contribute in making the very existence of the service possible, by paying part of the costs coupled to emitting television programmes. The same applies to advertisements placed on buses, which also contribute to paying a part of the service. Spam does the exact contrary: it slows the service (i.e. the Internet) down or at least overfills it with no usual information[9]. Spam thus constitutes a cost to the service, the cost being put on the recipient and on the network operators, without giving them value for money. Spam produces a real shift of costs, which is why it is very often seen as an illegitimate practice.

The cost-shifting argument (from the advertiser to the recipient) is the mostly used argument for qualifying spam as "bad". This is to the contrary of advertising in the real world, where the biggest part of the costs is borne by the advertiser. The persons targeted by the advertisement will see the advertisement, throw it away (in case of a paper found in his mailbox) or just look away (in the case of a television or road-side advertisement), or even take notice of the advertised product. In any of these cases, the costs incurred by the target of the advertisement are extremely limited, if not nil.

In cyberspace, things are different: there is no real target population; every user is indiscriminately targeted, regardless of his identity[10]. Advertising a product in cyberspace is very simple: all you need is a pretty basic computer with an Internet connection and a large number of email addresses to send the advertisements (i.e. the spam) to. Generally, these

---

[9] David E. Sorkin, *Technical and Legal Approaches to Unsolicited Commercial Email*, 35 U.S.F. L. Rev. 325 (2001), p. 336, available at: http://www.spamlaws.com/articles/usf.pdf

[10] see Edwards and Waelde, *Law and the Internet*, p. 311

email addresses will either be collected on websites where people often make them public too easily and are then exposed, or they will be bought from a competitor or any other company. The most brutal method is the compilation of email addresses by software which puts people's names from lists of existing names and surnames together with known domain names[11], to obtain potential email addresses which will then be spammed. Incorrect email addresses will not entail any costs, and generally the spammer will not even care, indicating a fake reply-to address[12].

The cost-shifting argument has lost a little of its original intensity. The analysis was extremely sensitive in older times, where Internet connections for most users meant dial-up connections through a phone line. In that case, the user had to first download the (potentially) large number of spam messages before even being able to delete them, meaning that a lot of his time online was taken up, resulting in him paying the connection for downloading spam. In the end, it is the user who takes up on him the distribution costs for spam. With the arrival and establishment of broadband internet connections, this scenario is not exactly true anymore as the connection time and volume become more and more close to unlimited. But spam has nowadays become a nuisance, which makes recipients incur costs to get rid of this nuisance.

Recipients have two solutions:

- the first would be to go through the messages manually and deleting those that do not appear relevant, be it to his business or for his personal purposes.
- The second would be for the user to invest in a so-called spam filter. These filters generally eliminate messages they consider as spam. However, these systems are not fail-proof and a large number of messages may simply slip through their controls[13] or they may delete messages that could have been important to the user. That's why a large number of these systems put the messages in a "quarantine" where the user can check if any messages have been lost. This may result in the user wasting time again, as he has to check his quarantine for any emails wrongly filtered out.

[11] Such as "hotmail.com" or "aol.com"

[12] Edwards and Waelde, *op. cit., p. 313*

[13] Especially because spamming techniques become more evolved by the day, always preceding the evolution os spam filters

The cost-shifting argument can be further elaborated: costs are not only shifted to the recipient of the message. Spam is a nuisance to the internet community as a whole[14]. The large volume of spam sent everyday has to circulate through the internet and as such is causing traffic congestions, overloading servers and taking up "valuable" storage space[15]. The general effect of this is that the speed of the internet as a whole is slowed down, causing damage to the internet community (i.e. the users of the internet taken as an entire group).
All of this means that, with the amount of spam increasing every day, email will soon become impossible to use, as it will cost more time than it actually was meant to save. A recent article even claims that email will die out if the levels of spam continue to increase[16] in the near future.

Some spammers repeatedly try to argue that automatic spam filtering is actually infringing their right to free speech. This argument can be quickly dismissed, however. A good example is set by a US case, Compuserve v. Cyber Promotions[17]. In this case, the defendants, in order to avoid an injunction being ordered, claimed that their right to free speech would be infringed if they did not have the right to spam any further. The judge was quick to dismiss their argument, holding:

"Defendants raise First Amendment[18] concerns and argue that an injunction will adversely impact the public interest. High volumes of junk e-mail devour computer processing and storage capacity, slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel, and cause recipients to spend time and money wading through messages that they do not want. It is ironic that if defendants were to prevail on their First Amendment arguments, the viability of electronic mail as an effective means of communication for the rest of society would be put at risk. In light of the foregoing discussion, those arguments are without merit."

---

[14] Edwards and Waelde, *op. cit.*, p. 312

[15] This argument has to be considered with care, as storage space is not anymore as rare a good as it used to be

[16] McFeelme Johnsons, *Email is dead, long love spam: Killer app is close to death*, available at: http://www.theinquirer.net/?article=16648

[17] United States District Court, SD Ohio, 3 February 1997, 962 F. Supp. 1015

[18] The First Amendment to the US Constitution establishes freedom of speech

It becomes evident that the free speech argument cannot operate efficiently and needs to be dismissed right away.
Considering that it is now established that spam should be regulated if not even prohibited, a legal definition of spam now needs to be given.

II. A legal definition of spam

Giving a legal definition for a technical phenomenon is never an easy task. This also applies to spam. Different legal instruments have tried to come up with such a definition, but most of the definitions only encompass the commercial form of spam, whereas a large number of messages containing scams which are not necessarily commercial in nature may well be treated as spam such as, for instance, the West African 419 fraud[19].

A good starting point can be found in the definition given by the French CNIL[21], which goes further than limiting spam to commercial email:

> *"spamming is the practice of sending unsolicited email, most frequently of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact, and whose email address was found in a public space on the Internet, such as a news group, mailing list, directory or web site."*[22]

An easier and simpler way to express this is to consider spam as:

> *"Unsolicited (commercial) email (**"UCE"**) from a sender you don't know".*

---

[19] This fraud is named after the section of the Nigerian Criminal Code which incriminates it. In general it will be an email (it used to be a letter some ten years ago), stating that a person has lost a relative in Nigeria (or any other African country), which has left behind a large amount of money, which now needs to be moved to another country. The scam is based on the idea that the victim will advance a certain amount of money as a guarantee, which will never be returned. More info on this fraud can be found at:
http://www.met.police.uk/fraudalert/419.htm

[21] Commission Nationale Informatique et Libertés, the French IT Regulator

[22] Report on Electronic Mailing and data protection, Commission Nationale Informatique et Libertés (CNIL), France, adopted on October 14, 1999 (**" the CNIL report"**)

However, I think that the definition should not be restricted to email, but broadened to any form of electronic communication, a definition which would then include spam sent over SMS[23]. The EU chose this way by adopting Directive 2002/58/EC[24] (**"the Directive"**): although the Directive does not directly refer to the word "spam", there is a general consensus that one of its objectives is to fight spam. The Directive[25] defines as electronic mail any *"text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is connected by the recipient"*. This is, of course, a very broad definition, yet this broadness may be of great help in fighting spam, as it does also extend to SMS messages. In brief, the Directive considers as spam any unsolicited electronic mail sent for direct marketing purposes. Again, the directive stops short of encompassing the full range of messages that can be considered as spam, by limiting itself to commercial messages which have been sent for direct marketing purposes. It seems clear that messages such as the West African 419 fraud would not fall under this definition, which is regrettable.

The United States has gone down the same road in the Can-spam Act 2003 which applies only to unsolicited commercial email.

Given the shortcomings of the current legal solutions currently in existence, I find that a fully-fledged definition of spam should go further than only including the sending of UCE. Rather, the definition should be extended such as to encompass email of pornographic nature[26], and it should also include scams such as the Western African 419 fraud.

In short, a definition for spam should consider as spam a message having the following characteristics: it is unsolicited, sent in bulk, and the content of the message presents some features:

---

[23] Short message system, the system for sending text messages over mobile phones

[24] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[25] Article 2 (h) of the directive

[26] Although this type of spam generally falls under the definition of commercial email

– **Unsolicited:**

The message is unsolicited if the recipient has never asked for the message to be sent to him, nor has he given his email address to a company for the purpose of receiving advertisements. Generally recipients' addresses are collected from websites where their address is published, or by generating random email addresses to which spam is sent[27].

– **Sent in bulk:**

This is probably one of the most important characteristics of spam. The bulk character of said message means that is set to a very large number of people, without actually the intent of reaching them personally. The only intent of the sender of the message is to reach as large a number of persons as possible, without having any specific target population.

– **The content of the message:**

This is the part of the definition where divergences arise: there seems to be a general tendency that the definition of spam should only be limited to messages where the content is of a commercial nature. De facto, this would exclude any scams like the 419 fraud (cf. supra), but also calls for funds from charitable organisations using exactly the same technique as spammers. This is, in my eyes, not the appropriate road to take, the definition of spam should go much further than just commercial mails. Otherwise the problem of overcrowded mailboxes will never be solved. There may, however, be problems with this, as jurisdictions, such as the EU, for instance, fight spam under the "consumer protection" label[28]. In this case, only commercial emails can fall under the sought prohibition, as scams or fundraisings do not fall under consumer protection.

As far as the content of the messages is concerned, the legislator will have to decide whether he wants to limit his action to pure consumer protection and as such eliminate (or at least try to) only a part of the spam that is sent everyday or whether he wants to solve the spam problem entirely in a single shot by generally outlawing messages that can fall under a broader definition of spam. There is, of course, always a risk that private mailing lists (especially of charities raising funds via email among their members) could fall under this definition. However, this problem will not be a real issue as their lists will become legitimate through the opt-in policy I am arguing for later.

---

[27] cf. *supra*

[28] The Directive has been adopted under art. 95 of the treaty, which allows the community to legislate in the matters of consumer protection

In summary, the definition of spam that should, in my eyes, be adopted, would be a very broad one including the three elements described above. To avoid that this could lead to a downturn of commercial activity by cancelling the efforts that have led to making the internet a commercially interesting environment, I suggest that the emailing of commercial messages should be made legitimate by implementing a strong but efficient opt-in policy: in other words, spam would by presumption be illegitimate, unless the recipient has agreed to receiving it in an informed manner[29].

As a a conclusion to this part, I suggest that messages falling under the following test should be considered as spam:

A message is spam if: it has been sent to a user without his consent or without him soliciting the message and if it has been sent in bulk to a very large number of such users and the content of the message is one of the following:

It is a commercial message

It is a scam, fraud or other incentive to take up a criminal activity

It is of pornographic character

It contains a call for the raising of funds

Having given elements that a good and elaborated definition of spam should contain, I wish to address the issue of how to implement the prohibition of spam into legislation.

III. Fighting spam

A. Fighting spam with existing laws

In this section I will give examples on how to fight spam with existing laws, taking from French and US examples.

In France, the first step was initiated by the CNIL report[30]: this report intends to fight spam on the grounds of violation of the recipient's privacy. It claims that it is illegitimate to collect email addresses from Internet sites, these addresses often containing personal information about the recipient (e.g. his name and country of origin). The report then proposes to apply existing privacy laws to spammers violating these provisions. This cause of action will certainly be very efficient, but will probably not apply to free email accounts (e.g. hotmail), as

[29] cf. infra for a more extensive development of this issue

[30] cf. *supra*, notes 3 & 4

users of these accounts often use a nickname, resulting in there being no personal element in their email address, and spammers sending unsolicited emails to this address could not be prosecuted on the grounds of violation of privacy. Yet these email accounts make up for a large part of the spammed email addresses.

The second step was initiated by the Tribunal de Grande Instance the Paris[31], which, in a civil decision, referred to the Netiquette[32] for declaring spam as an illegitimate activity. The facts were as follows: Mr P V was the user of free Internet accesses provided by LIBERTYSURF and FREE. Both companies cancelled his accounts after having warned him a few times, on the grounds that he used them for spamming. He sued both companies for damages for disrupting his Internet access. The judge held, dismissing the claim, that spamming was considered as an illegitimate and gravely disrupting practice on the Internet, and that as such it was contrary to the Netiquette[33].

Similar situations have appeared in the United States, where, before the Can-spam act, spammers were brought to court.

The first such situation was in Arkow v. Compuserve (1995), where Arkow sued Compuserve for having received unsolicited commercial advertisements by them. Arkow's argument was based on the prohibition of sending unsolicited facsimile advertisements. Unfortunately, the case never reached a full trial as it was settled out of court[34]. Moreover, it seems now that his action would probably have been unsuccessful, as in a 2002 case, the Pennsylvania Superior Court ruled that spam does not fall under the prohibition of the sending of unsolicited commercial faxes contained in the Telephone Consumer Protection Act[35].

---

[31] Tribunal de Grande Instance de Paris, Ordonnance de référé, 15 Janvier 2002

[32] The netiquette is a set of rules that are commonly agreed by Internet users as applying to life on the internet. It is a contraction of "net" (an abbreviation for the internet) and "etiquette" (which is a set of rules that describe adequate behaviour in a society. The netiquette is quite an abstract set of rules with the number and substance of rules varying from one internet community to another. There are however some concepts that remain the same such as respect of other people's bandwidth and storage space, which is the most important rule with regard to spam. A good example of rules contained in the netiquette can be found at http://www.albion.com/netiquette/

[33] *« Attendu que la pratique du SPAMMING, considérée dans le milieu de l'internet comme une pratique déloyale et gravement perturbatrice, est contraire aux dispositions de la charte de bonne conduite. »*

[34] For more details on this case and on some following cases, see: Sorkin, *op. cit.* , available at: http://www.spamlaws.com/articles/usf.pdf

[35] Aronson v. Bright-Teeth Now, No. 1179 WDA 2002 (Pa. Super. Ct. 2003).

Subsequently, other cases have arisen, but generally, they concerned service providers suing spammers for using their services in their spamming activities.

The most recent and probably most successful (except for the spammers) of these cases is **America Online, Inc. v. CN Productions, Inc. and Jay Nelson[36].** In this case, AOL was granted almost $7 million in damages federal district court to from a spam case. AOL originally filed suit against CN Productions in 1998 for sending a billion spam emails to AOL's subscribers. AOL was then awarded $1.9 million in damages and an injunction prohibiting further unsolicited e-mail. As the defendants had violated the terms of the injunction, AOL sued again in May 2001. The injunction was reaffirmed and AOL was granted the impressive amount of $7 million in damages.

In general, as a defence, spammers relied on the First Amendment, i.e. the free speech defence (cf. supra), but their defences have (until now), never been successful.

From this, we can see that existing laws can be used to fight spam. I believe, however, that too much uncertainty remains and that a new body of law should be created to address the spam problem.

B. Fighting spam with new laws

Creating new laws to get rid of spam seems to be a necessity. As I have suggested before, a good anti-spam law should encompass a general prohibition of sending email that falls under the definition of spam, with an exception where the recipient has opted to receive advertisements over email. This means that I am advocating an opt-in system as opposed to an opt-out system (1). Then there is the question of whether legislation should integrate a private right of action (2), the issue about how much corporations should be protected (3) and finally how this legislation may be enforced (4).

1. Opt-in or opt-out?

Basically there are two systems for regulating spam: the opt-out and the opt-in systems, the latter being the more restrictive one.

a. The opt-out system

[36] E.D. Va. 2002

In this system, email users, in order not to receive any unsolicited bulk emails, will have to be given the opportunity to object to being sent any spam. There are different ways for implementing this system:

A first one would be to create an opt-out registry containing a list of people who do not want to receive unsolicited email. This system would be built on the same basis as the registers of people who do not want to receive advertisement over telephone. There are however two problems with this system: the first is that it would have to be built on an international basis in order to be efficient, which is impossible in practice: if, technically, this system can be built, it will not be enforceable, as every State in the world would have to implement legislation to prosecute spammers disrespecting the system, which is absolutely fictitious. The second problem is that it relies on spammers' honesty, i.e. that they will have to respect the privacy of the people contained in the register[37]. A possible solution to overcome this would be to make the register inaccessible to the spammer. This would mean that the spammer would send his advertisement to the server running the register, which would then filter out the addresses of the people that do not want to be spammed and would then pass the message on to the others. There is however a strong security issue with this system: in the case of a leak, the spammer would be able to obtain the addresses contained in the do-not-spam database. With this, the opt-out system would be effectively set out of order.

The second way is to rely on companies' honesty to ask customers if they want to be excluded from future commercial mailings. The problem is that this option will often be very well hidden on a web page and formulated in a way that consumers will not really know what will happen if they check the box: will they have opted out or opted in? Further, this does not prevent "rogue" companies from collecting email addresses on web pages and spamming them.

A final point is that spammers often pretend to offer this possibility by offering a link in their mail where the recipient may choose to unsubscribe from their list. It turns out however, that these links are generally misused by spammers for confirming email addresses and on-selling them. Indeed, if this link is clicked, this shows that a human reads the address and as such it is a valid email address which can be sold to another spammer for good money. Given the frequency of cases where this has happened, most recipients have lost their trust in the value of the opt-out system, which means that, in my view, this system cannot be implemented

[37] National Do Not Email Registry: A report to congress, Federal Trade Commission, June 2004, p.15, available at: http://www.ftc.gov/reports/dneregistry/report.pdf. The **"FTC report"**

efficiently in any way. In other words, if legislation implements an opt-out system, there is a risk that recipients will distrust it and prefer to engage in self-help to be sure to be protected against spam. In the end, this would mean that the cost would still be shifted to the recipient, with an additional cost being put on the different countries for the setting up and maintenance of the do-not-spam register. As a matter of fact, the problem that should have been solved, the cost-shifting has not been solved at all, but worsened.

b. The opt-in system

This system is the more restrictive for spammers but probably also the more efficient one.
It requires companies wanting to engage in the sending of large amounts of emails for commercial purposes to require the prior consent of every recipient, before even starting the mailing. This can, for instance, be done during a sale of goods, where the company will ask the buyer if he wants to receive mailings about the company's activities.
Some sellers of goods over the internet already use the opt-in system[38]. There is however a great danger that this system is used in bad faith: a very common example is that there will be two check boxes on a website you are giving your email address to. The first will claim that if you do want to receive their email newsletters, you will have to check the box. The second will be a little more subtle by often stating:"check this box if you do not want your email address to be sold to a third party". This will, of course, confuse the customer, who will simply check the two boxes without thinking and thus exposing himself to a new wave of spam. This can be countered by stating that businesses must give their customers a clear choice, in bona fide. The above explained practice should be expressly condemned.

The opt-in system will prove to be by far the more efficient one for stopping unsolicited emailing, as long as it is implemented on an international basis. However, it will entail a large cost for companies acting *bona fide*, as they will have to review their marketing strategies in order to implement this system correctly. Finally, this system may also turn out to render legitimate marketing practices more complicated and expensive for these very companies

In order to implement both systems efficiently, the wild collecting of email addresses needs to be prohibited and harsh penalties need to be provided for against wrongdoers.

---

[38] Or at least they purport that they do not sell the email addresses in their possession, which is always difficult to monitor

2. Private right of action

A private right of action is considered by most consumer unions as a necessity in order to be able to fight spam efficiently. I do share this view, as it allows a broader way of action against spam, for instance it might make it easier to get back to spammers. Further, spam victims will be able to obtain compensations for the damages they experienced, which can be very high if we are talking about large firms being the victims as thousands of their email addresses receive thousands of spam messages a day and thus which slows down network traffic and consumes technical and human resources. Including a private right of action into a provision that intends to fight spam is essential[39].

3. Protecting corporations

Should corporations receive the same protection as individual users do? This is a broadly discussed issue, especially as the Directive allows the individual member states to decide on this point, forcing Member States only to make sure that corporations are sufficiently protected[41]. The argument that is usually given is that corporations do have enough financial and technical means to defend themselves[42]. This is why most legislative systems tend to adopt an opt-out system for corporations. However, I disagree with this conception. By focusing on the argument that the recipient has to bear the costs of emails (including server maintenance), it becomes obvious that corporations do also have to bear these costs and there is no reason why they should receive a protection that is less efficient than the one granted to individuals. This is especially true because large corporations suffer enormous losses because of spam, as they have to invest in spam filters, which have material and human costs[43].

---

[39] This opinion is also shared by the CAUCE, the Coalition Against Unsolicited Commercial Email (www.cauce.org)

[41] Article 13 (5) of the Directive

[42] In the case of the Directive, the main reason why they are excluded is that it is a Directive adopted under the consumer protection provisions of the Treaty. Companies are not normally regarded as consumers and as such cannot be protected.

[43] These systems need to be maintained in some way, and their filtering has to be checked, to avoid that important messages are filtered away.

4. Enforcing legislation:

Penalties will have to be created in order to enforce this legislation anti-spam legislation efficiently. These can range from civil damages to fines and even to imprisonment. The problem with enforcement of legislation lays with the fact that it only applies to one single jurisdiction. This causes special problems with respect to spam: Ii will be very difficult to legislate against spam coming from jurisdictions which do not have anti-spam legislation at all. If theoretically it is possible to incriminate spamming from another country[44], in practice, prosecution will be very difficult as it will be impossible to enforce e.g. a British criminal judgment in another country against a defendant who probably will never have appeared in Court. But this should not be a reason not to create anti-spam laws. On the contrary, it should give countries an incentive to work together and create similar anti-spam laws and collaborate in enforcing them.

C. Solutions found in the different jurisdictions:

1. Europe

The directive has chosen an opt-in system[45] by imposing prior consent to be given before commercial email can be sent. However, there is an exception to this very far-reaching rule: commercial email may be sent without prior consent to persons with whom the company has an existing customer relationship and if similar products are concerned. In these cases, the opt-out rule applies. As there are still some uncertainties about the existing relationship and similar products rules, mainly regarding interpretation, the British Department of Trade and Industry[46] has released a report commenting on these (**"the report"**):

a. Existing relationship

---

[44] As there will be an offence on British ground, where the recipient is spammed. There will, however, always remain complexities because of the truly cross-border nature of the internet.

[45] Article 13(1) of the Directive. This system only applies to individuals, as the Directive only provides for an opt-out system for commercial email sent to corporations. However, the individual Member States may choose to provide corporations with the same protection as individual users.

[46] Department of Trade and Industry (DTI), Consultation document, Implementation of the Directive on privacy and electronic communications, March 2003

The report raises the issue that an existing customer relationship may also include prospective customers who have shown an interest in a product and therefore have registered their email address. The report considers it as legitimate to include this type of customer relationship into the definition of existing relationship, as long as there are enough safeguards provided for, such as the fair collection of these email addresses, clear customer information and a chance for recipients to object to the use of their address. The report also asks for a direct relationship between the two parties for this exemption to apply[47].

b. Similar products

The DTI asks for a broad definition of similar products in order not to infringe too much on legitimate marketing practices. Again, it calls for enough safeguards to be established and asks companies to be fair in their use of this rule. The DTI also refers to the fact that there still is an opt-out rule if the companies were going too far. It remains complicated to define what similar products would be and this question remains an open one for a judge to determine.

c. Other provisions

The directive does not clearly provide for a private right of action, as it leaves this choice to the Member States by asking them to implement judicial remedies. Finally, the directive asks Member States to provide for judicial remedies where its provisions have not been respected, and clearly states that they should impose penalties on any person, whether governed by public or by private law, who fails to comply with these provisions[48].

2. United States

The United States have recently experienced a change in their ability to fight spam, with the adoption of the Can-spam Act of 2003[49]. This Act is a very controversial piece of legislation, as it is generally said to be more of a how-to-spam user's guide than a law to curb spam.
First of all, the Act does not introduce a general prohibition on sending spam and it is limited to emails with commercial or pornographic content. Under the Act, consumers have the right to ask a spammer to cease sending commercial email to their address and the spammer will

[47] ibid, p.37

[48] §47 of the preamble of the directive

[49] The long title is of the Act is "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003". This federal Act overrides all individual State legislation that may apply to spam.

have to comply with that request. In other words, a spammer will always have the ability to fire a first round of spam at a consumer, which is already a sign of weakness of the Act. It also requires all commercial email to carry a label stating its commercial nature and to indicate a return address that really exists[50].

It is also an offence to collect email addresses from protected computers[51]. The act does, of course, include penalties, reaching from fines to imprisonment.

However, the act generally permits the sale of lists of email addresses, except the sale of addresses that have opted out from receiving further commercial email.

In general, the Act creates an opt-out system and gives the FTC[52] the right to establish an opt-out registry at federal level[53]. The FTC has, however, already expressed its objection to the creation of such a system and, in a report to Congress[54], it explicitly states that it believes that such an opt-out register will not help in reducing the level of spam, but that it will actually become a very valuable tool for spammers to verify the validity of email addresses in their possession. The FTC has finally decided not to create such a registry. The CAUCE[55] has expressed mixed feelings on this decision, agreeing on the one hand with the FTC that a national do-not-spam register is not a good solution, that this will not stop spam. But, on the other hand, CAUCE expresses regrets, because this will effectively mean that the Can-spam Act will have no real practical use at all. CAUCE concludes that the only possible solution for Congress is to go back to the drawing board and draft an Act that has real teeth by implementing a prohibition on spam[56].

Further, the Can-spam Act does not contain a private right of action to consumers. Whereas this is very unfortunate, the Act has however created a right of action for service providers to sue spammers. However, empirical evidence has shown that the service providers do not obtain the intended result. A relatively recent article[57] shows that spammer prosecutions under

---

[50] s. 5 of the Act, see also: *Mixed reception on US laws to curb email spam*, Financial Times, 24 November 2003

[51] s. 4 of the Act

[52] The Federal Trade Commission

[53] s.9 of the Act

[54] FTC report, cf. *supra*, n.37

[55] Coalition against unsolicited commercial email, see http://www.cauce.org

[56] See http://www.cauce.org/news/index.shtml for the comments of the CAUCE on this issue.

[57] Thomas Greene, spammer prosecutions waste time and money,
http://www.theregister.co.uk/2004/06/16/spam_suits_dont_work/

the Act are a ruinous business for service providers, as litigation costs can rise up to $2 million for the Internet Service Provider seeking to sue, under the Act, a single spammer sending only a small part of the daily spam. Further, it is very difficult to actually find out who the spammers are, therefore large amounts of time and money will have to be spent to find the spammer and bring him to court. Generally this means that first there will have to be "John Doe" lawsuits, as ISP's cannot find the spammer. Only after these suits are filed can subpoenas be issued to identify the alleged spammers. In the end, this means that ISP's will not waste their time and money on trying to enforce the Act, but will probably prefer looking for technical solutions to fight spam[58]. This means that we are back to the starting point, with the Act having cost some ISP's a huge amount of money but hardly any result being reached. In the end, this means that an important part of the enforcement of the Act will simply not happen.

Conclusion:

Spam is a real problem, but it remains very difficult to legislate efficiently against it. This should nevertheless not lead us to refrain from passing any legislation at all, as it is only in making the first step that results can be achieved. Therefore, a strong commitment is needed by the European Union, to fight spam. Indeed, the EU has a very large moral authority around the world and if it innovates by introducing strong anti-spam laws, there is a great probability that other jurisdictions will follow. When it comes to fighting spam, the battlefield has become global.

As legislation will very often prove to lack efficiency because it will never be adopted on a world-wide scale, there will always remain some countries spammers can hide in and send their mailings from. However, if large countries such as the US or groups of countries such as the EU adopt anti-spam legislation, it is for sure that they will set a moral precedent which other countries in the world will feel bound to follow.

The fight against spam can also be fought on a completely different scale, at the individual user level, who can try to avoid publishing their email addresses on the Internet, or publish them in such a manner that an electronic address collecting system cannot collect them[59]. The original email address can easily be decompiled from the “encrypted” one by a human user, the task will be more difficult for a piece of software.

---

[58] *ibid.*

[59] e.g. create addresses like john@do.not.send.spam.hotmail.com

An eye should also be shed on more advanced technical solutions. Where the internet is concerned, technology has often proved to be more efficient for regulating than law. As Lessig puts it: in cyberspace, code (i.e. technology) is law[60].

With the appearance of spam filters, technology has made a great step forward in reducing the nuisance caused by spam. However this technology still does not prevent the cost-shifting that is inherent to spam. Since then, new ideas of how to cope with the problem have arisen. One of the most recent proposals was made by Microsoft and it consisted, basically, in creating a stamp charge for emails. The stamp would not be in the form of money, but in the form of computing time: before sending an email, a person's computer would have to do a calculation that would last around 10 seconds per recipient. This would render spammer's businesses uninteresting as they would lose an immense amount of computer time in calculations. However, the idea also has downsides, as legitimate senders of mail to a large number of recipients will also be penalised[61]. Although this technological solution does shift the costs back to the sender, some problems remain, such as who would be responsible for the supervision of the system. Since the internet is a worldwide phenomenon, it is hardly imaginable who could be the right person for regulating this. Internet Service providers seem to be good candidates, but it is always possible that there will be some service providers that will not play the game, leaving the system with a gigantic loophole which will surely be exploited by spammers.

As a conclusion, neither law nor technology left on their own will be able to provide us with a panacea to the spam problem. It is only if both complement each other that a solution may be found. There remains however one very efficient solution to spam lying in the change of some people's attitudes. The spam business model is only interesting because a large number of people do take up the offers that are presented to them. If people reacted more intelligently and stopped taking up these offers, this would effectively upset the spam business model and thus eliminate spam.

---

[60] Lawrence Lessig, *Code and other Laws of cyberspace*, p. 6

[61] For more information on Bill Gates' suggestion, see:
http://edition.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/

References

Textbooks

Roy V. Leeper and Phillip Heeler, *Commercial Speech in Cyberspace: the junk email issue*, in Susan Drucker and Gary Grumpert (eds) Re*al law @virtual space: communication regulation in cyberspace*, Cresskill, NJ, USA, Hampton Press 1999, pp. 349 – 370

Lawrence Lessig, *Code and other laws of Cyberspace*, Basic Books 1999

Lilian Edwards and Charlotte Waelde, *Law and the Internet: a Framework for Electronic Commerce,* Oxford Portland Oregon 2000

Ian Lloyd, *Legal Aspects of the Information Society*, Butterworths, London 2000

Articles

McFeelme Johnson, *Email is dead, long live spam*, June 2004, available at http://www.theinquirer.net/?article=16648

David E. Sorkin, *Technical and Legal Approaches to Unsolicited Commercial Email*, 35 U.S.F. L. Rev. 325 (2001), available at: http://www.spamlaws.com/articles/usf.pdf

Reports

National Do Not Email Registry: A Report to Congress, Federal Trade Commission, June 2004, available at http://www.ftc.gov (US)

Electronic Mailing and Data Protection, Commission Nationale Informatique et Libertés, Report adopted on 14 October 1999, available at http://www.cnil.fr (France)

Consultation document: Implementation of the Directive on privacy and electronic communications, Chapter 6, Department of Trade and Industry (DTI), March 2003 (UK)

Legal instruments

Can-Spam Act of 2003 (US)

Directive 2002/58/EEC 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 (Directive on privacy and electronic communications (OJ L201/37 of 31 July 2002) (EU)