Erasmus Law and Economics Review 1 (February 2004): 23–45.

AN ECONOMIC ANALYSIS OF SPAM LAW

Dennis W. K. Khong
Multimedia University, Malaysia
and
University of Strathclyde, United Kingdom.

Abstract

In this paper, I develop an economic argument for regulating the sending of junk emails, and examine the efficiency of various approaches to regulate junk emails. The first part of the paper develops an externality model of spam to show that in the absence of regulation, junk emails are inefficient. Next, I analyse the regulatory approaches presently used in the United States in three categories: opt-out, filtering and blocking, and opt-in. The study finds that spam can be both a positive externality as well as a negative one. However, the likelihood of being a negative externality is more probable. Absence regulation, no allocation of a property right to spam leads to an efficient level of spam. An examination of the three categories show that only the opt-in approach ensures that there is no net social loss, but not necessarily at a socially efficient level of spam. Hence, it is only a second best solution. Based on the conclusions that opt-in is the best solution given the constraints of transaction cost, the paper suggests a set of policy conclusions that serve as guidelines for countries enacting laws to regulate junk emails or spam.

Keywords: Spam, Junk emails, Unsolicited commercial emails, Unsolicited bulk emails, Information services, Externalities, Cyberlaw, Internet law.

JEL classification: K39, D62.

1. Introduction

Junk emails, also known as spam, are phenomena common to all email users. The uneasiness of email users to junk emails is apparent from the numerous state laws

© 2004 Dennis W. K. Khong. Subject to ELER Public License 1.0.
URL: http://www.eler.og

passed in the United States to regulate this aspect of Internet communication (Khong 2001; Sorkin 2001). In the European Union, a detail study of the impact of junk emails was recently carried out under the direction of the European Commission (Gauthronet and Drouard 2001).

In this paper, I develop an economic argument for regulating the sending of junk emails, and examine the efficiency of various approaches to regulation as proposed in the United States laws. It is divided into three parts. In the first part, I develop an externality model of spam to show that in the absence of regulation, junk emails are inefficient. Next, I analyse the regulatory approaches from two dimensions: first from the default allocations of property right in relation to spam: opt-out, opt-in, and self-help; and secondly, the three aspects of the 'cathedral': property rule, liability rule, and inalienability (Calabresi and Melamed 1972). Finally, I derive some policy conclusions based on the findings of this research.

2. Economics of Spam

To understand the economics of spam, we examine two models: one from the social welfare perspective, and another from a spam recipient's view. In the first model, there is only one spammer with many recipients of his spam; in the second, an email user receives spam from many spammers and some other emails.

2.1 One Spammer, Many Recipients

We assume a network with one spammer (*S*), one email service provider (*E*), and *z* number of homogeneous spam recipients (*R*) who each receives one spam email each from the spammer. The assumptions of one spammer and one email service provider, and homogeneous spam recipients,[1] simplify the model without significantly distorting the understanding when the assumptions are weakened.

The spammer's benefit is determined by the number of emails sent, z in this case, and the expected response rate for his mailing list, denoted by μ, where $0 \le \mu \le 1$. μ is an indicator of the success of his spam, measured by the number of contracts entered pursuant to his spam. This is also a function of how proximate is the interest of the recipients to the subject matter of the spam.

[1] The homogeneous assumption applies only in respect of marginal costs and benefits of spam but not preferences.

Hence, if the spam recipients are homogenous, μ can be increase by send spam emails which are more relevant to the recipients. If the spam recipients are not homogenous, two further ways to increase μ are, first, systematically removing recipients who individually have an expected response rate below μ, or, secondly, doing the same but by holding z constant, i.e. substituting a recipient who has a lower μ with a recipient who has a higher one.

2.2 The Spammer

The spammer derives utility B_S by having successful responses to his emails. The spammer incurs a cost C_S for getting the z email addresses with μ expected response rate and for the sending of spam thereto. C_S is the spammer's private cost of spam for z units of spam, where $C_S^{'} > 0$, for all z and μ.[2] Thus the cost of spam is given by $C_S(z,\mu)$, which is increasing in both z and μ. $B_S(z,\mu)$ is the expected benefit of the spammer, assuming $B_S^{'} > 0, B_S^{''} < 0$ for all z and μ. The utility function of the spammer in its most general form is given by

$$U_S = B_S(z,\mu) - C_S(z,\mu). \tag{1}$$

With no incentive to internalize externalities, the wealth maximizing spammer solves

$$\underset{z,\mu}{\text{maximize}}\, B_S(z,\mu) - C_S(z,\mu). \tag{2}$$

The first order conditions for z and μ, respectively, are given by

$$\frac{\partial B_S(z^{\circ},\mu)}{\partial z} = \frac{\partial C_S(z^{\circ},\mu)}{\partial z} \tag{3}$$

$$\frac{\partial B_S(z,\mu^{\circ})}{\partial \mu} = \frac{\partial C_S(z,\mu^{\circ})}{\partial \mu}. \tag{4}$$

2.3 The Recipients

Since the recipients are assumed to be homogenous, the expected benefit of each spam recipient is given by μB_R and the marginal cost of downloading and processing each email C_R. The utility function for one email recipient $r \in R$ is

[2] It is further assumed here that $z > 0$ and $\mu > 0$, for otherwise no spam email is sent.

$$U_r = \mu B_r - C_r \,. \tag{5}$$

The aggregated utility function for z number of spam recipients is

$$U_R = z\mu B_r - zC_r \,. \tag{6}$$

2.4 The Email Service Provider

We assume the email service provider incurs purely an average cost of C_E for each spam email received by his subscribers, and no benefit.[3] Therefore for z users, his utility function is

$$U_E = -zC_E \,. \tag{7}$$

Since z is exogenous to both the actions of the recipients R and the email service provider, we can combine their utility functions to make

$$U_{R+E} = U_R + U_E \,. \tag{8}$$

There are three possibilities for U_{R+E}: $U_{R+E} = 0$, $U_{R+E} > 0$, and $U_{R+E} < 0$. Taking $\mu = \bar{\mu}$ when $U_{R+E} = 0$, we get $\mu > \bar{\mu}$ when $U_{R+E} > 0$, and $\mu < \bar{\mu}$ when $U_{R+E} < 0$. It goes without saying that $U_{R+E} > 0$ when $\mu \approx 1$, and $U_{R+E} < 0$ when $\mu \approx 0$.

2.5 Welfare Analysis

Putting equations (1), (6), and (7) together, we get the welfare function

$$W = B_S(z,\mu) - C_S(z,\mu) + z\mu B_r - zC_r - zC_E \,. \tag{9}$$

Based on the Kaldor-Hicks criterion, the socially optimal level of activity and response rate, z^* and μ^* respectively, are given by maximizing equation (9)

$$\underset{z,\mu}{\text{maximize}}\, B_S(z,\mu) - C_S(z,\mu) + z\mu B_r - zC_r - zC_E \,. \tag{10}$$

The first order conditions for z and μ, respectively, are given by

$$\frac{\partial B_S(z^*,\mu)}{\partial z} - \frac{\partial C_S(z^*,\mu)}{\partial z} + \mu B_r - C_r - C_E = 0 \tag{11}$$

[3] Linearity is assumed here when the cost receiving and storing emails is a small fraction of the total cost of providing Internet services to its subscribers.

and
$$\frac{\partial B_S(z^*,\mu)}{\partial z} + \frac{U_{R+E}}{z} = \frac{\partial C_S(z^*,\mu)}{\partial z} \tag{12}$$

$$\frac{\partial B_S(z,\mu^*)}{\partial \mu} + zB_r = \frac{\partial C_S(z,\mu^*)}{\partial \mu}. \tag{13}$$

2.5.1 Optimal Number of Spam Emails

We compare equations (3) and (12), for any given μ, and derive Figure 1. Corresponding to the three regions of U_{R+E}, we have three possible ranges of optimal number of spam, z^*:

- When $\mu > \overline{\mu}$ and $U_{R+E} > 0$, spam is a positive externality. The socially optimal level z_h^* is higher than the private wealth maximizing level, z°.
- When $\mu < \overline{\mu}$ and $U_{R+E} < 0$, spam is a negative externality. The socially optimal level z_l^* is lower than the private wealth maximizing level, z°.
- Only when $\mu = \overline{\mu}$ and the net external effect of spam is zero, the private wealth maximizing level z° aligns with the socially optimal level z^*.

Put in another way, given that no regulation exists, only when $\mu^\circ = \overline{\mu}$, will $z^\circ = z^*$, and no market failure exists. At all other times, when $\mu^\circ \neq \overline{\mu}$, a market failure exists when z° is the number of spam.

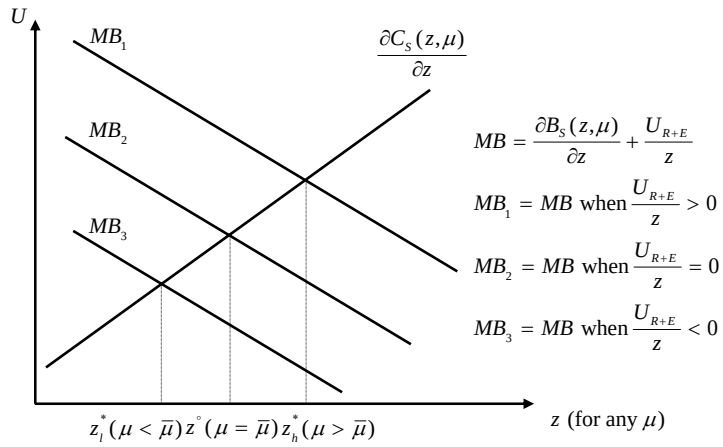

Figure 1

2.5.2 Optimal Level of Response Rate

Similarly, we can compare equations (4) and (13), and derive Figure 2 for any given level of z, where $z > 0$ and $B_r > 0$.

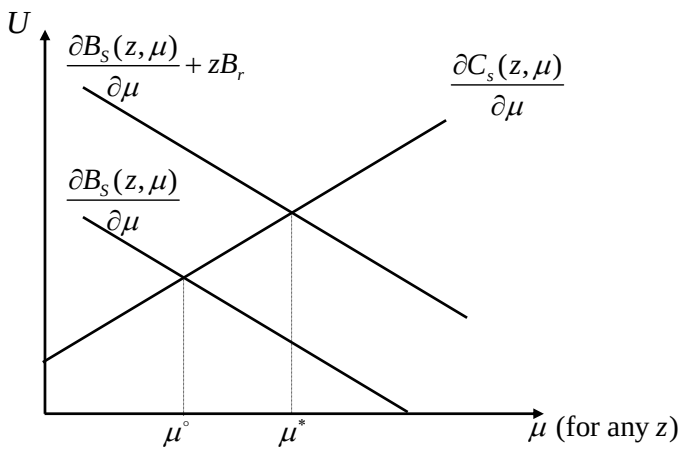

Figure 2

Figure 2 shows, that given B_r as constant and positive, the deviation of μ° from μ^* is proportionate to the number of spam emails, z. Hence, for any positive number of spam email, $z > 0$, the socially optimal level μ^* is higher than μ°. This is an important result, because it shows that in the absence of regulation, the privately wealth maximizing level of μ is always by definition socially sub-optimal.

2.6 Coase Theorem and One View of the Cathedral

In his seminal paper published, Ronald Coase (1960) showed that if the initial entitlement of property rights is clearly defined, and assuming no transaction cost, the final allocation of the property right is always efficient and the same, irregardless of the initial entitlement. This declaration later came to be known as the Coase Theorem. The normative version of this theorem suggests that since the final allocation is always the same, the initial entitlement should be as such which minimizes transaction cost, broadly defined, to promote efficiency. In respect of spam, this indifference of an outcome as suggested by Coase has to be recognized, as the right to spam or not to receive spam is a form of property rights.

Using the result and assumptions by Coase, Calabresi and Melamed (1972) discussed three protective forms of property rights, which they termed property rule,

liability rule, and the inalienability rule. A property rule protects property rights through an injunctive remedy, while a liability rule allows the infringement of property rights on payment of damages assessed by the courts. The authors further note that some property rights are limited in their tradability, i.e. they are protected by an inalienability rule.

It follows that under the assumptions of zero transaction cost and complete information, a socially efficient level of spam z^* and μ^* will be achieved, regardless of the initial allocation of property right, i.e. spammer having a right to spam, or email users having a right not to be spammed. Therefore, the more interesting question is to examine the situations where bargaining is impossible and parties do not have complete information.

2.6.1 Spammer Has a Right to Spam, Protected by Property Rule

We now consider the equilibrium where the spammer has a right to send spam, which is protected by a property rule, and negotiation between recipients and the email service provider is impossible, and parties do not have complete information. A wealth-maximizing spammer will first try to spam under the conditions of equations (3) and (4) where z° number of spam with mailing list of μ° expected response rate will be sent. At these levels, the externality is

$$U_{R+E} = z\mu B_r - zC_r - zC_E \,. \tag{14}$$

As indicated above, equation (14) may have three possibilities. When $U_{R+E} \geq 0$, from a Kaldor-Hicks perspective, there is no social loss. However, a socially undesirable wealth-shifting exercise occurs, when $\mu^\circ < \bar{\mu}$ and $U_{R+E} < 0$, the recipients and the email service provider suffer a net loss, but the spammer achieves maximum expected benefits.

If sending spam cannot be prohibited, social cost is minimized when μ is set to 1. Alternatively, $\mu \approx 1$ when an opt-in mechanism, as advocated by the anti-spam proponents, is adopted. In an opt-in mechanism, recipients have a right to legally prohibit the sending of unsolicited spam. Hence, when an email user voluntarily opts into a mailing list, his μ is likely to be 1 or near to 1.

2.6.2 Spammer Has a Right to Spam, Protected by Liability Rule

When the spammer has a right to send spam, which is protected only by a liability rule, theoretically, potential recipients and the email service provider, or anyone for that matter, may pay the spammer, to the amount equivalent to the lost opportunity from spamming, to stop the spam. No excessive or punitive sanctions can be granted against the users or the email service provider.

If the judge can accurately assess the expected net benefit of the spammer, and litigation cost is not prohibitive, like the preceding right protected by a property rule, the spammer will send spam at the privately wealth maximizing levels of z° and μ°.

If courts systematically overestimate the expected benefit, the spammer will send more than z° spam emails, and sue spam-blockers for damages. Conversely, if courts systematically underestimate the expected benefit, the spammer will have to lower his $B_S(z,\mu)$ accordingly and send more than z° spam with less than μ° expected response rate. On the same note, if the liability rule is not effectively enforceable, a wealth-maximizing spammer will send at the same levels as when damages are underestimated.

It is indeed difficult to imagine how this property right could be implemented on the Internet. Calabresi and Melamed (1972) pointed out that even an astute legal scholar such as Professor Frank I. Michelman (1971) omits discussing such a rule in his nuisance paper.

2.6.3 Users Have a Right Not to be Spammed, Protected by Property Rule

Conversely, when email users have a right not to be spammed, which is protected by a property rule, spammers are prevented from sending spam without a prior contractual relation.

Since the number of spammers is far lesser than the number of email users, spammers could induce email users to consent to their receiving spam by either paying them so (Jupiter Communications (2001), or ensuring that the expected benefits of spam to recipients are always positive. Consenting spam recipients will maximize their expected benefit of spam by selecting spam mailing lists which yield the highest μ. In order words, an opt-in scheme is used.

This does not take into account the costs of the email service provider. In a competitive environment, the email service provider will extract an amount equivalent to the additional cost of spam emails from its subscriber email users. This will be reflected in the cost of going online and having email services.

Alternatively, the email service provider may choose to contact spammers and extract a sum equivalent to the cost of running an email service. In this free email service, email users are willing to receive a controlled number of spam from the spammer to the extent that $U_R = 0$.

2.6.4 Users Have a Right Not to be Spammed, Protected by Liability Rule

When email users have the right not to be spammed, but are only protected by a liability rule, they can only claim damages from the spammer after they have been sent the spam. In this case, only users who suffered a net loss will be able to claim damages. Similarly, if the email service provider has a corresponding right, he will also claim damages. This will induce the spammer to send spam to the socially optimal level at conditions (11) and (13) and pay damages from his profit. Naturally, when transaction cost is zero, litigation cost is not prohibitive, and courts could accurately assess damages, a right not to be spammed coupled with a liability rule is efficient.

However, when claiming damages is difficult, such as when there is high cost of detecting the spammer, there will be a socially inefficient level of spamming. Spammers will send at the privately wealth maximizing levels of z° and μ°. Then liability rule is not efficient. This problem can be partially corrected by awarding higher damages than the value of the actual damage.

2.7 One Recipient, Many Spammers

Now, we examine the model where there is an email user I and many spammers are sending spam to his mailbox. In this case, x is the total number of emails received, and τ the probability that each email yields a positive benefit where $0 \le \tau \le 1$. $\tau B_I(x)$ is the expected benefit of emails, where $B_I^{'} > 0$ and $B_I^{''} < 0$ for all x. $C_I(x)$ is the cost of receiving and processing the emails. The utility function of the user is given by

$$U_I = \tau B_I(x) - C_I(x). \tag{15}$$

For any given τ, the optimal number of emails x° is given by

$$\tau \frac{\partial B_I(x)}{\partial x} = \frac{\partial C_I(x)}{\partial x}, \tag{16}$$

here U_I is maximum when $\tau = 1$.

An email address or mailbox can be viewed as a form of commons, or more aptly an open access regime (Ciriacy-Wantrup and Bishop 1975). The owner I could not prevent spammers or anyone for that matter from sending emails to him. Thus, each email increases x and the cost $C_I(x)$ increase correspondingly. However, when junk emails or spam exist, owner I could only benefit partially thereof. Like Garrett Hardin's (1968) open pasture, an email account may be subject to excessive abuse to the extent that users are forced to stop from using it (ReturnPath 2001).

$C_I(x)$ is composed of two types of cost. One cost is the telecommunications, opportunity cost of time, etc. associated with downloading each email. The analysis of this has been discussed in the preceding part. The second type of cost can be termed as 'second order' cost. This second order cost arise when an important email is missed in the flood of junk emails. Also, there is a risk of incurring unnecessary cost because of acting upon misleading junk emails or activating a computer virus transmitted through the spam email.

2.8 Spam as a Market Failure

A market failure exists when there is a divergence between social and private costs and benefits. Accordingly, when transaction cost is not zero, a spammer having the right to send spam will send an amount of spam z° which in most cases is not the socially optimal amount z^{*}. He will also under-invest in improving the expected response rate of his mailing list, i.e. μ° instead of μ^{*}.

Conversely, when email users have a right not to be spammed, protected by a liability rule, there might still be an inefficient amount of spam, especially when rational apathy among spam recipients causes them not to claim damages from the spammer, or when courts have difficulty ascertaining the actual amount of damages.

When email users have a right not to be spammed, protected by a property rule, opt-in mailing list will appear. Although the same socially optimal number of spam z^{*} and expected response rate μ^{*} will still not be achieved, because of the

transaction cost of opting in, the problem of negative externality is avoided when users have high μ and $U_R > 0$. Nevertheless, this positive externality is still a form of market failure when external benefits are not fully internalized.

3. Economic Analysis of Spam Law

Having answered the first research question on how spam is a market failure, the following sections analyze the regulatory approaches described earlier in chapter 3 using the tools of microeconomics. These regulatory approaches will be studied under the rubric of three categories — opt-out, filtering and blocking, and opt-in — with the conditions of transaction cost, imperfect information, and when there is rational apathy on the part of spam victim-recipients, high evidential and litigation cost, and high enforcement cost.

Under the opt-out category, we look at the requirement of true routing and header information, valid email addresses, provision of opt-out instruction, one-time spam, and the use of national or industry-wide opt-out registers. In the second category, we discuss the provision of filter-friendly identifiers, email service provider filtering, SMTP banner notification, and email service provider blocking. Thirdly, under the conditions of non-verifiability of true costs and benefits, we examine prior consent and revocable opt-in options.

3.1 The Opt-Out Approach

The opt-out approach is based on a limited property right to spam on the spammer. The argument for supporting this proposition is that since spam is no different from normal emails, and, email users have already implicitly consented to receiving emails by having an email account, email users should not *ex ante* discriminate against spam.

The economic argument would be that, as long as spam is, *ex ante*, potentially a positive externality, yielding an expected net benefit to its recipients under the Kaldor-Hicks criterion, they should not complain, even though, for the reason of heterogeneity of preferences, some recipients yields a net loss in receiving the spam. The argument goes further that if a recipient actually yields a net loss, he could contact the spammer to be opted out of the latter's mailing list.

Missing in this argument are two components: the cost of opting-out, and the possibility of reselling the email addresses. A spammer may create technical and financial barriers to opting out. Further, when a spam recipient contacts the spammer

to be opted out, the spammer collects his email address and resells it to other spammers, on a higher value, because the recipient has indicated that he takes the effort to read his emails. Legislation adopting the opt-out approach focuses on reducing the cost of opting-out, but is virtually silent on the collection and resale of email addresses.

3.1.1 True Information

Legislation mandating true routing and header information and valid email addresses serves two purposes. First, it lowers opt-out cost, and secondly, it reduces negative externality from flames and bounce emails on third parties when false routing and header information are used in spam emails.[4] True routing and header information allows the spam recipients to easily identify the spammer and send a request for opting-out of the latter's mailing list.

Of course, regulation without sanction is of little effect. The first approach most laws take is to define spam as wrongful when the routing and header information, or return email address, is false. When spam is wrongful, recipients, email service providers, and any victim may claim statutory or punitive damages from the spammer. It is hoped that the availability of high statutory damages is sufficient to induce knowledgeable victims to seek out the spammer, and reduce the problem of rational apathy on victims. On the same note, spam legislation requires providing clear information to spam recipients on ways to opt-out to further reduce information cost.

Since false routing and header information bring more social harm than any expected benefit, legislation may prohibit the selling or distributing of software which allows forging of routing or header information for the purpose of sending spam. The idea that if these software are not easily available because of being outlawed, incidences of negative externality because of false routing and header information is reduced.

---

[4] Flames are emails containing angry words used to retaliate against the initial sender. Bounce emails are emails which are 'returned to the sender' because the recipient addresses are not valid.

3.1.2 Opt-Out Cost

Having information on how and to whom to opt-out only goes half-way to reducing opting-out cost. The other part of the cost is the cost of contacting the spammer. For example, a few states such as California and Missouri mandate using email or a toll-free telephone number for opting out. This prevents barriers to opting out such as having to post a letter or paying long-distance charges to achieve the same.

None of the United States state laws regulate the collection and resale of email address. Perhaps this is the result of a lack of data protection law in that country. When users perceive that their email address would be harvested in an opt-out request, the act of opting-out brings a further cost to the whole operation. The consequence is that the idea of opt-out becomes ineffective (Hambridge and Lunde 1999). Regulation on email address harvesting is discussed below under the topic of opt-in in the context of the European Union Data Protection Directive.

Another way of reducing opt-out cost is the idea of one-time spam. Under this scheme, all businesses are allowed to send spam to unsolicited potential customers once. The idea is that once the potential customers are acquainted with the offerings of the spammer, through the spam, they can voluntarily sign up for further mailings. Thus non-interested spam recipients do not need to incur an additional cost of opting out.

From an economic point of view, this one-shot scheme sounds novel. Referring to the model of a wealth-maximizing spammer in equation (2), each spammer would send spam at z° and μ° levels. However, there will be a social loss, when under the condition that spam is a negative externality, according to Figure 1, z° exceeds the socially optimal number of spam emails.

3.1.3 Opt-Out Registers

Opt-out registers represent another innovation by the direct marketing industry as a response to the threat of legislation. Though, at the present moment, only the state of Colorado and the E.U. Electronic Commerce Directive recognize opt-out registers. Based on the arguments of the direct marketing industry, the use of opt-out register is an effective way for reducing opt-out cost.

In this system, an email user would have to register his email address in an opt-out register to indicate his unwillingness to receive spam or unsolicited commercial emails. A spammer then is compelled by law, according to the language of the legislation, to check his mailing list against the register and weed out all registered email addresses before sending his spam. Therefore, in theory, only parties who have not opted-out, and potentially have a positive net benefit, will receive the spam.

Use of opt-out registers becomes more complicated when multiple registers exist in different jurisdictions. Then an email user will have to visit all the different opt-out registers to register himself. Naturally, if there is a demand, there might be a website which will offer the service to register on the subscriber's behalf.

Spammers, on the other hand, will have many opt-out registers to refer to before sending their spam, thereby increasing tremendously the cost of sending spam. When cost increases, even if spamming is efficient, the net welfare gain is reduced. It is possible, that a spammer need not visit registers outside his personal jurisdiction, if long-arm legislation does not apply. But then, there will be a social loss when an email address which is registered in an opt-out register is missed because of non-verification. There might also be a race to the bottom when spammers relocate their operations to countries which do not have an opt-out obligation.

3.1.4 The Problem of Opt-Outs

The central economic argument of the legislative provisions on the opt-out approach is cost reduction of the opt-out process. It does not take into account the possibility of a social loss when spamming is done inefficiently. Neither does it induce spammers to send spam in an efficient manner.

This leads us back to the weakness of the opt-out approach, that is, the problem of non-scalability (Coalition Against Unsolicited Commercial E-mail 2001; Scruggs and Anderson 1999). Suppose all businesses suddenly decide to use some mailing lists and start sending an email to every email user, while at the same time complying to opt-out laws, the whole Internet and email system would grind to a stand still because of the sheer number of emails in the network.

From an economic point of view, opt-out is only efficient under very strict conditions, when $\mu = \mu^{\circ} = \bar{\mu}$ and $z = z^{\circ} = z^{*}$. Given that both μ and z are impossible to be verified by third parties, and $\bar{\mu}$ unverifiable, the opt-out approach is almost always inefficient.

3.2 Filtering and Blocking

Recall that filtering and blocking are ways to adopt the "ignore it" approach. When spam is a negative externality to its recipients, email users will choose to lower their loss of time by filtering mechanisms. Similarly, email service providers may also lower the negative externality by refusing to relay spam emails. The economics of these mechanisms will be examined below.

3.2.1 Economics of Filtering

After the first few encounters of spam, a rational email user will form the conclusion that spam is mainly useless and proceed to hit the delete key instead of reading them in order to minimize his cost, C_r. The result is that his expected benefit of spam μB_r goes down to zero, and μ declines towards zero for the spammer. It then becomes a vicious feedback cycle spiraling downwards, and the marginal cost of improving μ gets very high.

Email users could further minimize C_r if filtering is automated. They get legislative assistance from compulsory labeling law, where email advertisements have to identify themselves with the phrase "ADV:" in the subject line of the emails.

When spam is filtered at the email service provider's level, $\mu B_r = 0$ for those affected email users. This further increases the number of wasted spam as well as the marginal cost of improving μ. This cycle is aggravated as long as the marginal rate of substitution of z to μ is greater than 1. Spammers will continue to send more spam to compensate for the decreasing μ, and thus cause more social loss.

In the short run, filtering works as a signal to spammers that spam does not work. But in the long run, it is not a credible signal because filtering also creates a social cost on the filtering agents. Further, the use of filtering implicitly becomes the cause of negative externalities of spam when the expected benefit of spam is not captured by spam recipients.

If the sanction for breach of the mandatory labeling requirement is sufficiently high, spammers are compelled to follow the requirement. However, as the above discussion goes, it will lead to more spam when spammers compensate lower expected response rate with more spam.

3.2.2 Economics of Blocking

An email service provider may choose to lower the negative externality of spam by refusing to relay spam emails.[5] Although this does not reduce the cost to absolute zero, it substantially avoids the cost of forwarding and storing of spam emails for their subscribers. When this happens, no spam emails, theoretically, are forwarded.

If there exists an optimal amount of spam emails from a spammer, z^*, blocking may constitute a quantitative restriction, thus preventing the attainment of this welfare-maximizing level. Then, there is a social loss.

Also, blocking may give rise to a social cost resulting from the risk of mistakenly blocking legitimate emails, i.e. false hits. In general, blocking does not lead to efficient use of spam emails.

This result is similar under the proposed SMTP banner notification.[6] If spam may be correctly identified using this scheme, the risk of blocking legitimate emails is minimized, but the effect of a quantitative restriction still holds.

3.2.3 Conclusion on Blocking and Filtering

To date, filtering and blocking are the most common type of anti-spam mechanisms employed on the Internet. The analysis above shows that these mechanisms do not automatically compel spammers to send spam efficiently. In the long run, there are an increased in social loss in the form of filtering and blocking cost, more negative externality from spammers to compensate for these tools, potential loss of benefits from spam, and loss from false hits to the recipients.

3.3 The Opt-In Approach

Under the opt-in approach, spammers do not have a right to send unsolicited spam, and this right is protected by a property rule. Taken that statutory or punitive damages are high enough to compensate for rational apathy, spammers are induced not to send

---

[5] Emails are normally sent through the Internet via multiple servers which relay the emails from one to another.

[6] SMTP banner notification is a proposed system for an email server to notify relaying servers that it does not accept spam emails.

unsolicited spam. Instead, spammers will advertise their mailing list to potential recipients in order to get their consent for receiving targeted spam.

Similarly, when there is no right to send unsolicited spam, unauthorized collection or harvesting of emails becomes a social waste. Hence, making such an act unlawful and protected under a property rule, as in the European Data Protection Directive, minimizes social loss, and is in harmony with the opt-in approach.

As for the utility function of spammer, equation (1) still holds. $\partial C_S / \partial z$ is the cost of getting one more subscriber through non-spam advertising, and $\partial C_S / \partial \mu$ the marginal cost of advertising for a more focused (and also fewer potential subscribers) mailing list. When the mailing list becomes sufficiently focused, and its coverage sufficiently fits the interest of an email user, meaning the expected utility of the potential subscriber $U_r \geq 0$, the email user will subscribe.

The negative externality of opt-in spam on the email service provider remains. If the email service provider could monitor this and pass the cost of C_E to the subscriber, this cost will be internalized by the email users in the form of service charges, and U_{R+E} is then fully captured by the latter.

Under the condition that advertising is costly, i.e. $\partial C_S / \partial z > 0$, the spammer will still maximize his wealth, by attaining the level of z° and μ°. Through a process of self-selection, email users whose $U_{R+E} > 0$ when $\mu = \mu^\circ$ will subscribe. All external costs of spam are internalized by these subscribers, and there is always a net welfare gain.

This welfare gain is not Kaldor-Hicks efficient, for if the spammer moves to the levels of z^* and μ^*, social welfare is maximized. If email users as a group could negotiate in a Coasean way with the spammer, an efficient outcome can be achieved. But because email users are a large and dispersed group, organizing them is costly. For the same reason, opt-in laws are not common because of the inability of email users to organize as a pressure group.

The result is the same if advertising yields increasingly returns to scale. Spam is still not social welfare maximizing, although welfare is increased compared to the previous case. This is so because the gains by subscribers are not internalized by the spammer.

The opt-in approach is only a second best approach because it ensures that there is no social loss through negative externalities. A Kaldor-Hicks efficient approach does not exist.

3.4 Remedies

One of the aims of legal remedies is to achieve optimum deterrence. Common types of civil remedies include damages and injunction. In addition, the state may take actions on behalf of victims through the penal system, with punishments such as a fine or a prison term.

In the spam context, remedies are used to compel the spammer to send spam at a socially optimal level. When the socially optimal level cannot be achieved because of unverifiability, as discussed above, the remedies are used to prevent a net social loss.

This remedial objective, however, suffers from two complications. First, because in a single spamming session many victim-recipients are affected, there will be a rational apathy and a free-riding problem when claimants may sue based on the action of the first claimant. Secondly, high evidential and litigation costs are involved in making a successful claim against the spammer. To bring spam closer to a socially efficient level, these remedies must be adjusted for these shortcomings.

3.5 Civil Remedies

The problems of rational apathy and high litigation cost may be corrected by awarding punitive damages, where the award is higher than the actual damage suffered. One form of punitive damages, as used in the U.S. state spam law, is statutory damages.

Punitive damages ordinarily should be awarded if, and only if, an injurer has a significant chance of escaping liability for the harm he caused (Cooter 1989; Polinsky and Shavell 1998). However, if a corporation is a separate entity and directors are not personally liable, this mechanism is not effective against corporations, because the principal injurer is the management while the ultimate bearers of any punishment are the shareholders and customers.

Statutory damages have another advantage, in that the problem of quantifying actual damage is dispensed with. This has the effect of lowering evidential and litigation cost.

Another solution to the rational apathy problem is to allow a class action. In a class action, one or more victims sue on behalf of himself and other non-litigant victims. Economics suggests that class actions are appropriate when the stakes are large in aggregate and small for any individual plaintiff (Cooter and Ulen 2000, 387).

3.6 Criminal Remedies

Apart from proving the actual harm suffered in quantitative terms, a plaintiff in an action against a spammer, must prove that the defendant is the right party, namely, that the harm was *caused* by the action of the defendant. This may require having sufficient technical expertise and evidential records from relaying network service providers. When these providers reside in foreign jurisdictions, calling these parties to give evidence may be prohibitively costly.

In this case, the state may be in a better position to pool resources from taxes to initiate a criminal action. Also, states may enter into multilateral treaties or arrangements with other countries to collect evidence for Internet-related litigation. The optimal punishment in the form of a fine then equals to the harm divided by probability of being sanctioned (Becker 1968).

3.7 Conclusion

The three approaches to spam are discussed. Opt-out spamming does not lead to a socially optimal level of spam, and likely to cause a net welfare loss through negative externalities of spam. Neither does the use of filtering and blocking. In fact, filtering and blocking do nothing more than increase the social cost of spam.

The opt-in approach always ensures a net welfare gain, and minimizes the welfare loss through the negative externality of spam. It is only a second best approach as it does not lead to a socially optimal level of spam.

Remedies have to be aggravated to compensate for incidences of rational apathy and high evidential and litigation cost.

4. Summary of Findings

Earlier, we find that under the condition of high transaction cost, none of the allocation of a property right to spam or not to be spammed leads of a socially

optimal level of spam. The exception is that under the very strict condition when the externalities of spam sum up to zero under the Kaldor-Hicks criterion.

In all other situations, spam is either a positive externality or a negative one, where being a negative externality is a more probably outcome. Externalities, in any case, are a form of market failure where the private wealth-maximizing level deviates from the socially optimal level.

Junk emails, examined from the point of view of a recipient, are a further social cost, when second order costs are taken into account. These second order costs arise in the form of risk of missing an important email in the flood of spam, and acting upon wrongful, misleading or harmful spam emails.

In the second part, we examined spam regulatory approaches under three categories: opt-out, filtering and blocking, and opt-in. We conclude that opt-out provisions are only concern with opt-out costs and do not induce the spammer to a socially optimal level. We further find that recycling of email addresses lowers the private cost of spam and leads to more spam being sent.

On the point of filtering mechanism, we find that it is not a credible device in the long run because it does not cause the spammer to internalize the negative externalities of spam, and only leads to more spam and social waste. Blocking is a more effective tool, but runs the risk of blocking legitimate emails and also preventing unsolicited emails which bring a positive benefit.

By far, the opt-in approach is better than the rest and can be termed the second best approach. Revocable opt-in spam induces recipients to internalize the social cost of spam, which can be offset by the expected benefit of spam. However, when advertising for opt-in mailing list is costly, a socially optimal level of opt-in spam is not achieved.

5. Policy Conclusions

Starting from the conclusion that the opt-in approach is the best available, for it minimizes social losses, we derive the following policy conclusions on spam.

1. Only opt-in advertisement emails are allowed. Unsolicited bulk or commercial emails are banned.

2. Opt-in mailing lists are revocable, and clear instruction and a cheap method of unsubscribing from the mailing list should be provided.

3. Subject lines must be non-misleading and properly identified. Standardized filter-friendly identifiers need not be used if unsolicited spam is illegal.

4. Relay blocking is allowed where it is clearly known that a particular sender or source is sending unsolicited spam. SMTP banner notification is not needed, since the default rule is that unsolicited spam is not allowed.

5. States should provide civil remedies in the form of statutory damages and punitive damages against unsolicited spam. In addition, class actions against unsolicited spam should be allowed.

6. States should have criminal remedies against spammers who intentionally violate the rule against unsolicited spam. At the same time, states should enter into a multilateral treaty to exchange evidence for violations of Internet laws.

7. Property rights in email addresses such as that respected in the Data Protection Directive should be preserved. Addresses collected in an opt-in mailing list should not be transmitted or sold to another party for any purposes without the consent of the subscribers.

8. Existing laws on consumer protection, advertising and the tort of misinformation should apply for liability from misleading commercial emails.

In this paper, we examined the incidence of spam based on a model of email communication. The conclusions derived therein rely on existing understanding of junk emails, limitation of technologies, and the regulatory approaches. Further research can be done on the empirical side of spam regulation as well as its applicability to new forms of spam such as wireless spam, location-sensitive advertisements to mobile phones based on Global Positioning System data, and instant messenger spam. It is hoped that this paper can be a guide to countries enacting laws to regulate spam.

Acknowledgement

This paper is part of a thesis for the European Master of Law and Economics programme in 2000/2001. The author thanks Professor Thomas Eger for kind supervision and the Multimedia University, Malaysia for financial support to the

author to complete the programme. Also, comments and corrections from the editors of the Erasmus Law and Economics Review are appreciated.

References

Becker, Gary S. 1968. Crime and punishment: An economic approach. *Journal of Political Economy* 76:169–217.

Calabresi, Guido, and A. Douglas Melamed. 1972. Property rules, liability rules and inalienability: One view of the cathedral. *Harvard Law Review* 85:1089–1124.

Ciriacy-Wantrup, Siegfried V., and Richard C. Bishop. 1975. Common property as a concept in natural resource policy. *Natural Resources Journal* 15:713–727.

Coalition Against Unsolicited Commercial E-mail. 2001. CAUCE does the math—Why can't the marketing industry? 15 May. Available from http://www.cauce.org/pressreleases/math.shtml.

Coase, R. H. 1960. The problem of social cost. *Journal of Law and Economics* 3:1–13.

Cooter, Robert D. 1989. Punitive damages for deterrence: When and how much? *Alabama Law Review* 40: 1143.

Cooter, Robert, and Thomas Ulen. 2000. *Law and economics,* 3d ed. Reading, Mass.: Addison-Wesley.

Gauthronet, S., and E. Drouard. 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. Available from http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spam.htm .

Hambridge, S., and A. Lunde. 1999. Don't spew: A set of guidelines for mass unsolicited mailings and postings (spam). Internet Society and Internet Engineering Task Force, June 1999. Request for Comments 2635. Available from http://www.ietf.org/rfc/rfc2635.txt.

Hardin, Garrett. 1968. The tragedy of the commons. *Science* 162:1243–1248.

Jupiter Communications. 2001. Marketers will pay to reach email users. 29 January. Available from http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356392&rel=true.

Khong, W. K. 2001. Spam law for the Internet. *Journal of Information, Law and Technology* 3. Available from http://elj.warwick.ac.uk/jilt/01-3/khong.html.

Michelman, Frank I. 1971. Pollution as a tort: A non-accident perspective on Calabresi's cost. *Yale Law Journal* 80:647.

Polinsky, A. Mitchell, and Steven Shavell. 1989. Punitive damages: An economic analysis. *Harvard Law Review* 111:869–962.

ReturnPath. 2001. New study reveals that consumers' email address changes undermine email marketing efforts. 30 January. Available from http://corp.returnpath.net/media/rel_013001.jsp.

Sorkin, D. E. 2001. Technical and legal approaches to unsolicited electronic mail. *University of San Francisco Law Review* 35:325–384. Available from http://www.spamlaws.com/articles/usf.pdf.

Scruggs, Derek, and Heidi Anderson. 1999. Sometimes the messenger should be shot: Building a spam-free e-mail marketing program. Available from http://www.messagemedia.com/.