Webology, Volume 3, Number 1, March, 2006

E-marketing, Unsolicited Commercial E-mail, and Legal Solutions

Xingan Li
Faculty of Law, University of Lapland, PL 122, 96101 Rovaniemi, Finland. E-mail: xingan.li (at) yahoo.com

Received February 18, 2006; Accepted March 30, 2006

Abstract

The purpose of this paper is to explore the legal solutions to unsolicited commercial e-mail. The advantages of e-mail enable it to be one of the most important e-marketing instruments. Spammers are also motivated by potential profits in spamming. The low costs and high benefits of the spammers, and the high costs and low benefits of the spammed determine the illegal nature of the spamming. The spam poses challenges for e-mail recipients' property rights, fair trade, public morals, cybersecurity, personal data protection, and involves other concerns as well. In dealing with spam, technical and marketing solutions cannot work alone without the legal mechanisms. The legal regulation is justified by balancing the interest between senders, service providers and even users. Criminal sanctions, civil remedies, and international harmonization are alternative steps in establishing legal solutions. As a necessary part of the legislation, punishment for unsolicited commercial e-mails should be more severe. Still, there are a number of limitations to the effectiveness of law enforcement against spamming. Spam must be eliminated by comprehensive mechanisms.

Keywords

Direct Marketing, Spam, Unsolicited Commercial E-mail, Legal Solutions

---

Introduction

With the development of e-commerce and the prevalence of the Internet, e-mail has become the primary means of communications and marketing. Compared with the traditional marketing tools, e-mail has obvious advantages. However, the abuse of e-mail disturbs the normal communications services, and influences the environment for the public to use the Internet. The reception of unsolicited electronic messages and commercial information become a pervasive social and economic problem. The difficulties in identifying the senders and in compensating the recipients' losses further prove the uncontrollability of the Internet. Spamming impedes the effective application of telecommunications to the individual and business communication, baffles the consumers' acceptance of legal e-marketing, and in turn, hinders the growth of the e-commerce. Many individuals and institutions are making efforts to seek solutions to the problem (for example, Coalition Against Unsolicited Commercial Email, 1999; Cobb, 2003; Direct Marketing Association; Federal Trade Commission, 1998, 2003; Ferguson & Piragoff, 1997; Gartner Consulting, 1999; Gauthronet & Drouard, 2001; Goodman & Rounthwaite,

2004; Hansell, 2003; International Telecommunication Union, 2004; Khong, 2001, 2004; Midnet Media, 2003; Mail Abuse Prevention System, 2004; Organization of Economic Cooperation and Development, 2003, 2004; Peppers & Rogers, 2000; World Summit of Information Society, 2003 and many others). In order to ensure the convenience of the Internet use and improve the security and efficiency of the Internet environment, some countries have implemented specific legislation to regulate spam; the European directives required the member states to incorporate commercial e-mail rules in the provisions on privacy and telecommunications. Organization of Economic Cooperation and Development (OECD) called for legislation and international cooperation in combating spam. Based on documentary analysis and empirical study, this paper explores the threats of the unsolicited commercial e-mail and the difficulties in dealing with the problem, analyzes the dilemmas in combating spam under the present legal framework, and suggests possible countermeasures.

Background and definition of spam

As the capability of computers and networks to process information increases, "a wealth of information" can lead to a "poverty of attention" (Simon, 1982). Unsolicited business e-mail (UBE) or unsolicited commercial e-mail (UCE) represents an example that e-mail users have to deal with the superfluous information they do not expect to consume. It is generally called bulk mail or spam. It turns out that spam has evolved into a large amount of information garbage, polluting the environment of e-marketing. When we talk about the phenomenon of spam, we are talking about a negative externality in e-marketing that people try to get rid of. It brings about the negative image of e-marketing, frightening e-mail users from trusting the e-mail communications.

Up to April 2005, the population of global e-mail users increased to 683 million, with almost 1.2 billion lively accounts. The e-mail marketing has been regarded as one of the most successful marketing means on the Internet (Niall, 2000). Unfortunately, with the increase of the e-mail usage, two thirds of the total 130 billion messages sent and received everyday are unsolicited (Radical Group, 2005).

In nature, e-mails can be a kind of information goods, for example, messages provided by the paid subscription services; while at the same time, e-mail can also be a kind of bads, in case the subscribed paid information are harmful to general public or to specific groups or a certain person. If the information is provided free of charge, it becomes an externality. When the messages are useful, they are positive externalities; when they are harmful, they become negative externalities. Whether they are with charge or without charge is decided by the sender; but whether they are useful or harmful, is decided by the recipient.

Nonetheless, spam sent out to multiple recipients, blemishes the name of e-mail marketing (Wreden, 1999; Wright and Bolfing, 2001). Institute of Management Technology (IMT) Strategies (2001) found that the e-mails that the users never read are increasing, and the consumers tend to constraint or interrupt the e-commercial contacts. Before the universal access to the Internet was available, the e-mail spam was really a small trouble. But today, most users worldwide are confronted with this problem nearly everyday. The problem has increasingly important influence on the consuming behaviors. In an InfoWorld article (2003), a survey disclosed that over forty percent of respondents answered unsolicited e-mail as the worst problem in the field of information technology industry in the previous year. The scale and effect of the spam prevalence implies that spam has become "significant and growing problem for users, networks and the Internet as a whole" (World Summit on the Information Society (WSIS) Declaration, 2003, paragraph 37).

Most people have some unclear awareness that spam at first came from the "spam skit by Monty Python's Flying Circus"[1] (Templeton, 2003). However, according to Templeton (2003), the history of spam can be traced back to the late 1970's with a number of network services that were sent multiple mailings, these initial group mailings were not considered annoying and as a result they got the chance of wide online spread (Templeton, 2003). Kelly (2002) explored the history of spam and believed that it was born on April 12, 1994. We can also reasonably judge that it was until the Internet was in its wide usage, when unsolicited e-mail posed a real threat.

The consensus on the definition of unsolicited e-mail is nearly reached among academia, legislature, and law enforcement, even though the actual legal practices are few. Mail Abuse Prevention System (2004) defined spam as:

"An electronic message is 'spam' if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender."

Although the definition of e-mail spam only denotes to the sender and recipient, they can be understood as covering individuals, organizations, enterprises, and public institutions. It is a common concern in local, national, and international layers. During the Geneva phase of the World Summit on the Information Society, spam was identified as a potential threat to the full utilization of the Internet and e-mail (International Telecommunication Union, 2004).

Classification of spam is vital from a legal standpoint, because most spam legislation targets a particular type, such as business e-mails, or deceptive spam. The United States Federal Trade Commission identified twelve most likely spam scams: business opportunity scams, making money by sending bulk e-mailing, chain letters, work-at-home schemes, health and diet scams, easy money, get something for free, investment opportunities, cable descrambler kits, guaranteed loans or credits on easy terms, credit repair scams, and vacation prize promotions (Federal Trade Commission, 1998).

The unsolicited e-mail being a central concern, spam can also come from other sources, such as newsgroups, mobile phones Short Message Service (SMS) and instant messenger services. The legal solution to these kinds of spam is possibly in common, and countries have laws to cover spam of these and other forms of media, but this paper is mainly concentrated on e-mail spam.

Comparison between traditional and e-mail advertisements

Besides interpersonal interaction through e-mail, e-mail has also broad usage in advertising as well. What accompanies the unsolicited commercial e-mail is that it parallels with the legal advertisements, that is, e-mail advertisements. To better understand the phenomenon of spam and find effective preventive mechanisms, the following section contributes to compare the advantages and disadvantages of traditional advertisements, particularly postal advertisements, and the e-mail advertisements (See Table 1).

Table 1: Comparison between traditional advertisements and e-mail advertisements

Compared Items	Traditional advertisements	E-mail advertisements
Public consciousness	Familiar	Unfamiliar

Scope	Indirectly attention-getting	Direct attention-getting
Basis of trust	Publicity	Confidentiality
Targeted audience	Mainly subscriber	Mainly non-subscriber
Censorship	Involving intermediary censorship	Lacking intermediary censorship
Costs	High	Low
Form of trade	Traditional form to traditional form	Electronic form to traditional form or electronic form
Sending and reply addresses	Provided, mostly the same	Provided or not, same or different
Receiving addresses	Limited territorial range. The wider the territorial range, the higher the costs	Unlimited territorial range. Costs independent of territorial range.
Jurisdiction on disputes	Easy to ascertain according to existing laws, regulations and cases.	Difficult to ascertain. Lacking ready laws, regulations and cases.
Regulation on spam	Yes	No
Possibility of regulation on spam	Easy	Difficult
Collection of evidence on spam	Converse investigation: from consumer to registered or licensed intermediary and advertiser.	Difficult to investigate. No such registration or license.
Deterrence of punishment on spam	Strong	Weak
Possibility of recommitment of spamming	Low	High
Effect of spam	As the increase of traditional advertisements, advertisers and intermediaries better off, while recipients better off, or no change.	As the increase of unsolicited e-mail advertisements, advertisers and intermediaries better off, while recipients will worse off.

The e-mail marketing has the following advantages:

- (i) Being directly attention-getting. In most cases, the e-mail advertisements are similar to traditional advertisements in the form that the audience are not strictly divided and designated, such as the advertisements in newspapers, magazines, radios, TV programs, outdoor advertisements, or even online banner advertisement. But the e-mail marketing has the high potential to provide personalized information according to the users' different needs, hobbies, and interests. It is not strange that a professor receives advertisements on conferences, sales of books, and so on; that a professor of economics receives more specified information on conferences on economics, sales of economic books, and so forth. Many other forms of advertisements do not have so concentrated an audience. Peppers and Rogers' study (2000, p 4) discovered that the one of the success factors enabling the e-mail marketing to work well is "high response rates." The average reply rate of e-mail is 5-15 percent versus 1-2 percent for direct mail and 0.005-1 percent for banner advertising, while the e-mail marketing creates a positive effect on branding efforts (Midnet Media, 2003, p.1).

- (ii) Interactive marketing. The e-mail marketing can keep more customers. The decrease of costs and timelines permits business to communicate with customers more frequently. Regular e-mail marketing to existing customers generates a 15-50 percent increase in overall online trade. Engaging customers in a two-way dialogue enhances customer satisfaction and yield quicker response (C.f. Sandiego Media Inc., 2005).
- (iii) Confidentiality. The contents of e-mail advertisements are not necessarily confidential. E-mail is not in itself the most confidential form of communications. But for a certain users in a certain environment, the e-mail marketing is like a consult or negotiation in a closed room. What the user decide to buy, to whom the user pays, and what and from which address the user receives, are not directly showed to anyone else. In case that the user consumes digital information, the e-mail and other electronic or online marketing might be the most suitable means.
- (iv) Low cost. The e-mail marketing lowers costs and increases profits. The e-mail marketing supplies cost-saving benefits, such as no printing, mailing or media expenditure; allows for more frequent customer conduct, which turns into higher income; average costs of 0.03 to 0.1 dollars for each e-mail, versus 2 dollars for direct post and up to 3 dollars for telemarketing; customer acquisition costs average no more than 24 dollars for e-mail versus 82 dollars for public relation, 958 dollars for print advertisements, and 1,457 dollars for radio advertisements (Midnet Media, 2003, p.1).
- (v) Diversified forms of trade. The e-mail marketing serves both traditional and digitalized goods. The goods are usually exhibited online. For traditional goods, though the electronic exhibition is not as intuitionistic as show window, or door-to-door marketing, the multimedia explanation may provide more comprehensive a presentation than any other forms of marketing. In case of digital goods, the e-mail marketing has the unique advantage in providing sample texts, and audio or video clips. In fact, many online book stores, music and video dealers, and software vendors all provide some kinds of sample to show their goods. The e-mail marketing can directly link to these online markets and goods.
- (vi) Location independent. The senders and the recipient of e-mails are both location independent. The senders can send e-mails from anywhere of the world to recipients located anywhere in the globe (if they are not outside the earth). Trans-border marketing is not limited by the national boundary. A nearly uncontrollable route realizes the flow of goods, particularly digital goods. Even if it is traditional goods, the uncontrollable information might also cause the traditional control of trans-national flow of goods more burdensome. All in all, the trans-territorial flow of goods can benefit greatly from e-mail marketing.
- (vii) Advertisers better off; and intermediaries might also better off. As a natural effect, with the increase of e-mail marketing, the advertisers will surely better off. The voluntary intermediaries will also better off, because a portion of the profits is transferred from the advertisers to the intermediaries.

The disadvantages of e-mail advertisement are:

- (i) Most people are less familiar with e-marketing than traditional advertisements. Less people are more familiar with e-mail marketing than traditional advertising. But more and more people are more familiar with the new advertisements than ever.
- (ii) Targeting both subscriber and non-subscriber. This may induce more consumers, but may also annoy e-mail users. In fact, different forms of traditional advertisements are designed to different audience. Some forms do not distinguish subscriber or non-subscriber, such as radio, TV and outdoor advertising. But traditional postal marketing mainly targets subscribers, together with newspaper and magazine advertising. With e-mail advertisements, the businesses can limit

marketing to subscribers, but can also extend to non-subscribers in order to get more profits. This advantage for senders becomes the greatest disadvantage for recipients.

- (iii) Lacking intermediary censorship. Unlike traditional advertisements that have been published on media that are managed by intermediaries, the e-mail marketing is actually direct marketing- more direct in the sense of business-to-consumer, but at the same time more indirect in the sense of no longer face-to-face. The necessary censorship on the process of information provision is missing. Subsequently, the transaction process is also less monitorable and less controllable.
- (iv) Sender's genuine identity and displayed information might be different. The falsification of sender's identity and address might mislead the consumer to open the unsolicited e-mail. The reply address might be invalid when the recipient replies to refuse further messages. The recipients have less choice in deciding whether or not to receive this kind of e-mail.
- (v) Lack of dispute solution mechanism. The possibility of regulation on e-mail marketing is law. The jurisdiction over disputes is difficult to determine. The laws, regulations, and rules, particularly international harmonization are not ready. In addition, collection of evidences is confronted with great obstacles.
- (vi) Weak deterrence of punishment on abuse of e-mail marketing. The spammers have high possibility of recommitment, motivated by monetary interests. As a result, the recipient might worse off due to absence of self-determination, while the intermediaries might also worse off due to the absence of profit transfer agreement.

The advantages and disadvantages seem more and more beneficial to the senders but less and less beneficial to the recipients. As a result, the senders have the stronger incentive to send more marketing e-mails, while the recipients have the stronger to receive less. The overuse of e-mail marketing by the businesses will lead to underuse by the consumers.

Challenges of spam to the society

The advantages of e-mail marketing greatly upgrade the utility of e-mail in business. Both the legal and illegal commerce discover this efficient instrument in harvesting money from the market. The following summarizes a list of common challenges of legal sense that the spam brings to the society.

The first challenge is against e-mail recipients' property rights. The spammer infringes the property rights through two ways. On the one hand, spammers usually transfer the cost of sending bulk e-mails to others, including individuals, e-mail service providers (ESPs) or Internet service providers (ISPs), for example, intrusion others' computers or servers to send e-mails, or evasion the reasonable fees payable to the service providers. On the other hand, spammers usually practice fraud and deception in spamming. Spammers disguise the origin of their messages so as to ensure that the users read their messages. Federal Trade Commission (2003) reported that 66 percent of spam messages are fraudulent in the "from" or "subject" lines, or in the message itself. For example, if the subject line includes the term such as "reply", "your required information", "your free laptop", "free travel chances", etc, it is highly possibly that the users will open the e-mail and find if these are valuable messages. As for the contents, many unsolicited e-mails offer various deceptive or misleading representations. The most common fraud schemes include the Nigerian scam, online chances of making money, and drugs sales, etc. In a successful detected case, the FBI in the United States and the Spanish police arrested 310 people who were the Nigerian conspirators of a bogus lottery scam involving 100 million Euros. The scam victimized more than 20,000 people in 45 countries (Libbenga, 2005).

The second challenge is targeted at fair trade. Contents of most unsolicited e-mails involve false advertisements or situation leading to misunderstanding. Due to the facility of

transfer, such e-mails incorrectly relay erroneous information, and mislead the recipients and consumers in the bargaining. Besides the breach of the regulations on consumer protection and constitution of criminal fraud, the false advertisements might distort the normal market of goods and services, harm the normal trade order, and reduce the consumers' confidence (Taiwan Ministry of Transportation and Communications, pp. 6-7).

The third challenge is offending public morals. Unsolicited e-mails are usually not targeting specific e-mail users, among which children are highly possibly to be harassed. Because the spam messages often contain contents inappropriate for children, such as the hyperlinks of pornographic websites, pornographic pictures, and adult entertainment products and services, the pornographic spam has become a public risk for the growth of the children. From the pornography industry revenue statistics, it is apparent that the Internet-related revenue has already reached a noteworthy scale. What is worse is that the average age of first Internet exposure to pornography is as low as 11 years old, and 90 percent of the children between 8-16 years old have viewed pornography online (TopTenReview, 2005).

A relevant problem is that in some East Asian and Middle East countries, creating, copying, selling, and spreading pornography might lead to arrest and conviction (See example, Penal Law of China 1997, Articles 363-367). In addition, merely possession, and browse of pornography is traditionally prohibited. The unsolicited e-mails make it difficult to judge whether the existing punishments are applicable to e-mail users who passively receive and "keep" e-mails with pornographic contents. For example, Management Regulations on Internet Online Service Business Location provides that the manager of Internet online service business location and the Internet users must not create, download, copy, view, release, spread or use by other means the information containing obscenity contents (China State Council Management Regulations on Internet Online Service Business Location 2002, Article 14).

The fourth challenge is a threat to cybersecurity. The security problems brought about by the spam generally require the interaction between the users and the messages. The large volume of spam, the malicious programs and malicious linkages contained in the messages are the main threats (PC World, 2003). In recent years, many of the most harmful malicious programs have been spread through exploiting e-mails.

The fifth challenge involves personal data protection. There is little exception in the available literature and legislation on spam that does not emphasize the identity theft. Many spammers send their messages by unauthorized use of other individuals or organizations' accounts (OECD, 2004). The e-mail addresses harvesting software can collect this information automatically from the webpages (Boldt, Carlsson and Jacobsson, 2004, p. 8). Therefore, the misuse of spamware and the collection and use of e-mail addresses are among the focuses of the legal regulation. If the e-mail address includes enough information to identify the user, the collection and use of such an e-mail address should under the consent of the user. Without such consent, the collection and use of the address in the spamming invalidate the privacy protection.

The sixth challenge is comprehensive. Besides the above aspects, spam is also involve in other content-related and goods-related transgresses and offences. The examples of the former category are online piracy of intellectual property, spreading of malicious programs and codes, defamation, slander, and libel, and so on. The examples of the latter category are sales of controlled goods, such as drugs, prescribed medicine, and weapons; providing services, such as auction, financing, tourism, dating, prostitution, gaming, gambling, raffling, bonus, and lottery.

In sum, at least at present, the ease of using spam to offer goods and services increases the volume of spam. Sophos statistics showed that global spam at the end of 2004 has reached 3 trillion messages, with an estimated cost of 131 billion dollars (EquIP Technology and Cipher Trust, 2004). In addition, according to an Industrial Development Corporation (IDC) study, worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC, 2005).

Costs and benefits of the spammer and the spammed

1. The costs and benefits of the sender

Whether the spammer send the spam is thought by economists as controlled by "the invisible hand"[2] of interests. According to Khong (2004), although it is difficult to measure the costs and benefits of the spammer, if the benefit obtained from the activity outweighs the cost, then the spammer will undertake the spamming activity. It follows that if there is one successful commercial transaction, the spammer can realize his/her benefit. The costs that are involved in the spamming can be roughly estimated in the following aspects:

First, bandwidth cost. It is inevitably to involve the cost of bandwidth in the message sending. According to Living Internet (2005), as a form of communication across global distances, e-mail is relatively the cheaper way. Based on a very conservative cost of 10 dollars a gigabyte for bandwidth, Living Internet showed that every 50 thousand e-mails cost one dollar in bandwidth costs. That is to say, the per message bandwidth cost is only 0.000020 dollars. If the spammers undertake these costs, the monetary investment will be very tiny compared with the possible income from the spamming.

Second, costs in sending message. Besides bandwidth costs, there are also other costs associated with sending a message. This is usually measured by how much the spammer is willing to do the spamming. According to Goodman and Rounthwaite (2004), the higher price is about 0.001 dollars per message, the lower price is about 0.000025 dollars per message. The cheaper charges range from 0.0001 to 0.0003 dollars per message.

Third, to obtain users' e-mail address may also involve some kinds of costs. But the actual cost may depend on the ways in which the addresses are harvested. According to Sadowsky, the spammer can obtain users' e-mail address in the 13 situations (Sadowsky et al., 2003, p. 55). But obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software. The software are also available from Internet, either free of charge or with an inexpensive price.

Even trickier, the revenue of spammer from sending message has been found high in a few studies. Goodman and Rounthwaite (2004) cited the following information in clarifying how much per message revenue would be. They cited that Grimes (2003) had reported one person had had the revenue of as much as 0.0005 dollars per message, but was willing to do as little as 1,000 dollars per mailing: as little as 0.0000125 dollars per message. Other information they cited was from a *Wall Street Journal* article, reporting that a person obtained 360 dollars or sending 10 million messages, around 0.000036 dollars per message (Moran, 2002).

The above information indicates that the costs of the spammer are increasingly low, while the revenue is increasingly high. Hansell (2003) found that compared to the cost of 190,000 dollars for one million conventional bulk-rate postal mails, the marginal cost of sending a marketing message to one million recipients by electronic mail is less than 2,000 dollars. He estimated that commercial e-mail is profitable if one recipient in 100,000 makes a purchase. The fact that the spam can be sent at very low cost and in a great

quantity has attracted direct marketing companies to use spam e-mails for advertisement. Cobb (2003, p.2) suggested the concept of "the parasitic economics of spam," meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message. In reality, some spammers pay nothing for sending their messages, hijacking resources that belong to others.

2. The costs and benefits of the spammed

The costs induced by the spam to the spammed have a wide coverage. They include the waste of the users' time, bandwidth and storage, cost of anti-spam solution, and cost of overloading at the mailbox.

First, the topic of whether the waste of time in dealing with the spam is disputable. Spam messages are annoying in that the users have to spend time and money dealing with them. In daily life, some people argue that they know e-mail well and it is easy to identify spam messages from useful e-mails. Even if there are some bulk mails, the user needs only a few seconds to browse the address, subject, content, signature, etc in making a judgment. To delete them is also not so complicated. They doubt how the problem can be so serious and so wasteful. In fact, meeting with messages well falsified in address and subject lines, the user is impossible to judgment whether this is a spam or a message from a contact. When the message is open, the user has to browse the contents and signature to make the final decision. If the message begins with information of his interests, the users have to spend yet more time to decide whether or not to delete the message. The average time and money lost in processing a single message might not be so significant. But the aggregate loss of time and money in aggregate taken in dealing with these messages might be huge.

The time the users spend on dealing with spam messages can be quantified in a way of counting numbers of messages the users receive everyday, and the time spent on making judgment on whether the messages are spam and deleting them. In some services companies, the treatment of these messages needs special care so as not to ignore the customers' requests, complaints, and business communications. EquIP Technology and Cipher Trust (2004, p.1) found that the average e-mail user receives up to 70 e-mails a day. According to Zeller (2005), a December 2004 survey suggested that Internet users spend an average of 10 working days per year dealing with spam, and at least some industry analysts estimated that the yearly cost of spam to business due to lost productivity and additional network maintenance costs will be around 50 billion dollars.

Second, spam also induces costs of the bandwidth and storage. Khong (2001) pointed out that in addition to the losses of the users, the spam also has great impact on e-mail service providers (ESPs). The European Union estimated the global bandwidth costs of spam at 8-10 billion dollars annually (EquIP Technology and Cipher Trust, 2004, p. 2). The potential threats might even severe to cause an ESP's network to shut down (Goodman, 2000). The interruption of services is unfortunate for both the providers and users in causing business, confidence, and other losses.

Third, the influx of spam has caused many people and organizations to deploy some form of anti-spam solution. A European Commission study estimated that the costs associated with these solutions might come up to 10 billion euros per year worldwide (Gauthronet & Drouard, 2001). Gartner Consulting (1999, p. 4) found that the longer an e-mail user kept an e-mail account, the more likely he would be spammed. It indicates that spam is a more severe threat to the established users than the new comers, and a more severe threat to the users more dependent than the users less dependent on e-mail. That is to say, the more possible the users benefit from the e-mails, the more possible they bear losses from spam. The increased profits of the spammer are just based on the increased loss of the spammed.

It is reasonable to deduce that the spamming business would growth in pace with the development of the e-commerce.

Finally, another side effect of the spam is that it corrupts e-mail services, fills up users' mailbox with useless information, and decreases the usefulness of the e-mail service. Even worse, if the e-mail address has ever been put on the institution's website, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by spammers. Under these circumstances, the number of spam messages might increase in an unexpected pace. I keep an e-mail address provided by a high profile website. It has been put to the Internet for a few occasions. Recently, the average number of spam messages per day may reach one hundred. Although the fortunate bulk mail prevention function by the provider works well, and most bulk mails are automatically put into the specific folder, sometimes, it is inevitable that useful messages are also identified as spam, and the inbox is still filled with dozens of spam messages everyday. Most of the spam messages can really be judged through the subject or address lines. To delete them needs a few seconds everyday. The most annoying is that it is really difficult to look for the useful messages from dozens of useless messages received unexpected. The final solution is to notice the contacts the change of the address.

In fact, from the analysis above, we can identify nothing useful and beneficial to the spammed. They undertake pure losses, not only the monetary, but also the psychological.

The limitation of technological and market solutions

The technical solutions to spam involve complicated mechanisms, which are not the primary concern of this paper. But the main means are filtration and blacklist. The former is used to filter the sources, headers, and content. The latter is used to mark the refused IP addresses. Practices proved that the technical filtration often misjudges, deletes, and blocks the useful and legal e-mails, and incapable to effectively stop sending of spam from the sources. At the same time, the technical solution also has influences on the transmission of the e-mail service providers and the terminals (Taiwan Ministry of Transportation and Communications, p. 13). It is also possible that the recipient install filtering software to prevent spam. But it is still less effective.

In the meanwhile, spam technology and anti-spam technology are competing in contesting with the market. The technical capacity of tracing spam source is always limited (Taiwan Ministry of Transportation and Communications, p. 14). Besides the economic incentive in spamming and the technical limitation in anti-spamming, the issue is worsened by the extra costs of the service providers on improving computing ability to filter the spam, and the potential risks of misjudgment and breach of constitution. If there is no legal warrantee and liability, the possible technical solutions might also be discarded. The technical solution could be effective only when certain legal basis is ready to divide the risks between the senders, the service providers, and the recipients.

Given the technological solution is not the unique way; the legal regulations on spam are further justified by the limitation of non-legal solutions. The following analyzes the disadvantages of the non-regulatory measures.

Theoretically, the prohibition of spam could be integrated into regulations on the protection of consumers' rights. But the traditional laws can at most extend privacy protection to the activities of misuse of mail lists according to the personal data protection law, such as in Taiwan. However, this protection is limited to eight industries and cannot provide complete protection for consumers (Taiwan Ministry of Transportation and Communications, p. 6).

Self-regulation is practiced by various coalitions of anti-unsolicited e-mails. The goal of these coalitions is focused on that the consumers enjoy the right to accept or refuse the bulk mails, and that the Internet resources and privacy should be sufficiently respected. The awareness of the consumers, website managers, and the Internet service providers helps to take coherent actions in combating spam, and enhancing the quality of Internet services.

Observing the current situation, we can find that the consumers' protection and self-regulation mechanisms are both less effective as well. On the contrary, the problem of spam is growing more serious. Therefore, clear rules are needed to define the scope of the spam and offer suitable punishment, neither throttling e-mail as an e-marketing tool nor leaving it as it is.

Legal regulations on spam

1. Basic approaches within the legal framework: opt-in vs. opt-out

In dealing with spam, various technological solutions are being created, used, and proved to be less effective. As a necessary remedy of the problem of the spam, legal framework must also be used to fight against spammers.

The first step in taking a legal action is to consider whether the consent of the address owner should be obtained prior to the sending of the spam message. If the prior consent is necessary, the method is called "opt-in". If the prior consent is not required, the method will be "opt-out".

The opt-in mode fully takes care of the free will in receiving messages. Through receiving e-mails, the recipients can acquire certain information. But the privacy of the recipients and the consumers must be taken into account. The right of privacy is now widely recognized and protected in constitutions and laws worldwide. Remedies for infringement of this right have also implemented through civil law or criminal law. Any potential threats to the privacy should be considered in advance of the activities. The opt-in mode might better serve this goal in the information age. Opt-in mode is adopted in Australia, China, and the European Union (for example in the United Kingdom).[3]

With Directive 2002/58/EC, the European Union has adopted an "opt-in" approach for commercial communications by e-mail. The Article 13 of the Directive titled "*Unsolicited communications*" provided that:

"The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent."

However, Article 13.2 also leaves an open door for a kind of special opt-out choice:
"Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use."

Article 13.3 explicitly limits the use of unsolicited communications for purposes other than direct marketing. They are not allowed either without the consent of the subscribers

concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. This provision ensures the effective opt-out in cases the users choose to interrupt the subscription after either opt-in or limited opt-out.

The general requirements in sending commercial e-mails are by the way of ensuring the real identity, and address. Article 13.4 of the Directive prohibits the "disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease."

The Article 13.5 of the Directive further provides that the subscriber in provision about the definition of unsolicited communications and the limited opt-out provision shall apply to natural persons. But it requires the Member States to sufficiently protect the legal interests of other subscribers.

The Directive helps to establish a legislative model within the framework of the European Union. Opt-in approach has been adopted in most EU Member States, and is under consideration in some other countries (Sipior, Ward and Bonner, 2004, p. 62). Under the opt-in approach, the burden is on the senders to offer the "opt-in" option. For the e-marketing as a whole, in the case of sending in goodwill, the user can save time and costs in processing the irrelevant messages. In the case of sending mala fide, the recipients can prevent in advance. The main advantages of opt-in e-mail services are timeliness, convenience, and control.

Compared with the opt-in mode, the opt-out mode considers the difficulty of the industry in acquiring the users' written consent. If the use of such information were prohibited, the industries of financing service, direct marketing, and customer credit would be directly impacted. The advantage of the opt-out mode than written consent is that it can balance the personal privacy and right of individual consumer, offering the opportunity for consumers to express their will on whether or not to receive specific category of e-mails. The opt-out mode is adopted in Canada, Japan, South Korea, Singapore, Taiwan, and the United States.[4]

In the North America, the United States CAN-SPAM Act superseded more than 30 state laws covering spam. The legislation adopts an opt-out approach under strict limitations. Section 5 of the Act provides the requirements for transmission of messages:

1. Prohibition of false or misleading transmission information. The Act outlaws sending commercial e-mail message, transactional or relationship message with header false or misleading information to a protected computer (Section 5 (1)). Even if the header information is "technically accurate", including the originating e-mail address, domain name, or IP address, but when they are obtained by means of false or fraudulent pretences or representations, they are regarded as "materially misleading" (Section 5 (1)(A)). If the sender "knowingly use another protected computer to relay or retransmit the message" in order to disguise the origin, the header information shall be regarded as "materially misleading" (Section 5 (1) (C)).
2. Prohibition of deceptive subject headings. The Act outlaws sending commercial message if know or should know that "a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message" (Section 5 (2)).
3. Prohibition of omitting return address or comparable mechanism (Section 5 (3)). The Act outlaws sending commercial e-mail message without displaying "a

functioning return electronic mail address or other Internet-based mechanism" (Section 5 (3) (A)). The Act further requires that the return address or other mechanisms can be used by a recipient to opt-out by the way designated in the message (Section 5 (3) (A) (i)). The return address must be available for "no less than 30 days" after sending the message ((Section 5 (3) (A) (ii)).

4. Prohibition of transmission of commercial electronic mail after objection. In the case of opting out by a recipient, then sending e-mail more than 10 business days after the receipt of such request is unlawful (Section 5 (4)).
5. Inclusion of identifier, opt-out, and physical address in commercial electronic mail (Section 5 (5)).

The effective opt-out mechanism should be "sending once, and identifying once." It means that the messages are sent to the recipients only once if the recipients do not receive such messages any longer, and the recipients need to identify the same source of the same messages only once before he/she decide to refuse or subscribe it. Under such circumstances, mode of the users searching information changes to the mode of the users judging whether the coming information is valuable. Thus it is less wasteful for both the senders and recipients, if the senders are sending the information in goodwill.

The disadvantage of this approach is that it increases the costs of processing information in distinguishing those useful from useless, wasting work time, human resources, and money. For overall comparison of these two means, see Table 2 below.

Table 2: Comparisons between Opt-in and Opt-out (Hong Kong Information Security Website, 2005)

Approaches	Advantages	Disadvantages
Opt-in	Burden on senders to offer opt-in option. Recipients save time and costs in processing irrelevant messages. Recipients prevent spam in advance.	Malpractice of some traders. Lead to insufficient, asymmetry information, and increase costs of information searching. Malicious senders join the mail lists, and send more specialized spams.
Opt-out	Burden on recipients to inform opt-out. Sending once, identifying once. Information searching changes to information selecting.	Opt-out becomes confirmation to spammer. Cost of processing information increases.

The distinction between opt-in and opt-out modes is easy to make. But in the case of opt-out mode, there exist a special case that needs a special legal answer. If the recipient of the opt-out e-mail sends back the message with selected items that he consents to receive or refuses to receive further e-mails, it is purely the purpose of opt-out. The recipient bears the expenses involved in the process. But if the recipient does not reply to the opt-out offer, the judgment of whether the recipient is willing to receive further e-mail cannot be made without an explicit legal provision. The law must give an indubitable answer.

2. Regulated scope of unsolicited message

The contents and categories of regulated unsolicited message vary among countries from each other. In the aspect of the contents of the regulated unsolicited message, countries generally target at commercial communications, such as in Australia, Japan, Korea, the United Kingdom, and the United States. The Australia Act on Unsolicited Electronic Information 2003 applies to "commercial electronic message," unless it is exempted. The Korea Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 defines unsolicited messages to

advertisement information for the purpose of earning profit or commercial advertisement. The United Kingdom Privacy and Electronic Communications (EC Directive) Regulations 2003 applies to e-mail sent for the purpose of direct marketing. The United States CAN-SPAM Act defines "commercial electronic message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." (Section 3 (2)) Hong Kong Bill against Unsolicited Electronic Message 2005 proposes regulation on unsolicited commercial electronic message. Non-commercial message, such as the communications of governments and citizens, contribution appeal of the charity or religious organizations, communications of political parties are not limited. The provision of China Management Measures on Internet E-mail Services 2005 is wide enough to cover all kinds of e-mail messages.

In the aspect of the forms of the regulated unsolicited messages, there are also different legislations. The law in the United States limits the message to commercial e-mail. Similarly, China also limits the form of spam to e-mail. The mobile message is excluded.

Other countries adopted broad legislation to outlaw more kinds of messages. The regulated electronic message in Australia covers e-mail, instant message, and telephone. The scope of the United Kingdom law covers automatic calling system, facsimile, and e-mail. The Section 5 of Australia Spam Act 2003 defines the purpose of the Act to regulate commercial electronic message including e-mail, instant message, telephone, and similar messages. But voice calls are excluded: If a message is sent by way of a voice call made using a standard telephone service, the message is not an electronic message. Korea outlaws unsolicited e-mail, telephone, facsimile, or other media prescribed by the Presidential Decree. The term "other media" is obviously used to cover short message service (SMS) and other electronic communications services. At the same time, Korea also specifies those messages sent to recipients in violation of law as spam (Personal Data Dispute Mediation Committee, Korea Information Security Agency, 2003, p. 5-6). The Hong Kong bill covers all the unsolicited commercial electronic messages: e-mail, facsimile, instant message, and multimedia message, messages generated automatically by devices, including audio or video messages recorded beforehand and sent through the Interactive Voice Response System (IVRS) (Xie, 2005).

3. Labeling of commercial e-mail

Labeling consists of displaying standard identifying labels in the subject line or header. Some countries require senders to label certain kinds of messages, but others do not require it (Ahn, 2004). In order to make it possible for the e-mail service providers and the recipients to distinguish and filter the e-mails before open them, the general provision requires the sender add some words in the commercial e-mails, such as "advertisement." China requires labeling of "Advertisement" in Chinese or "AD" in English. Taiwan Draft Regulations on Unsolicited Commercial E-mail requires labeling of "Commercial," "Advertisement" in Chinese or "ADV" in English. The bill also authorizes the agency in charge of the regulation to publish other labels that can be used to identify the commercial e-mail. In Korea, Article 11 of the Ordinance of the Ministry of Information and Communication of the Act (Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001) requires an "ADV" label. But in order to prohibit the irregular forms of labels such as "A*D*V" and "A~D~V", the Ordinance was revised in 2002 to exclude the irregular forms. The revision also requires an "ADLT" (adult) label if the e-mails are for adults. In June 2003, the Korea law further requires to "include the '@' (at) symbol in the title portion (right side) of any commercial e-mail address, in addition to the words 'Advertisement' or 'Adult Advertisement' as applicable." (Korea Information Security Agency, 2003).

Many states in the United States require a label in the subject line of an e-mail that will alert recipients that the message is an advertisement. This includes two modes: unsolicited sexually explicit messages must contain a label of "ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT" at the beginning of the subject line; unsolicited commercial e-mail messages must contain a label of "ADV:" or "ADVERTISEMENT". False, deceptive, or misleading subject lines are outlawed. Table 3 shows the different legislation modes on the problem of labeling in the United States (for a complete summary of the U.S. state laws, see Sorkin, 2006).

Table 3: Legislation Modes concerning Labeling

Legislation Modes	Categories	Label	States
Requirements of Label	Unsolicited sexually explicit messages	"ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT"	Alaska, Arkansas, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Missouri, New Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin
	Unsolicited commercial e-mail messages	"ADV:" or "ADVERTISEMENT"	Arizona, Colorado, Michigan, and Nevada
Prohibition of False, Deceptive, or Misleading Subject Lines			Arizona, Illinois, Indiana, Kansas, Maryland, Minnesota, Missouri, North Dakota, Oklahoma, Pennsylvania, South Dakota, Texas, Washington, West Virginia, and Wyoming

In order to avoid possible disputes and damages in the direct marketing through e-mail, effective tracing of senders is critical. Laws require the sender to provide correct header of the e-mail. The Section 5 (a) (1) of United States CAN-SPAM Act, Article 3 (3) and Article 5 of Japan Specified Commercial Transactions Law for Appropriate Transmission of Specified E-mails 2002 all provide the similar requirement. The sender's identity information is also an important requirement in commercial e-mails. The Section 5 (a) (5) of the US Act, and Article 3 (2) of the Japan Law both make such provisions.

In the United States, states have taken different steps to criminalize the act of sending unsolicited commercial e-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information; the sale, distribution, and possession with intent to sell software that is designed to falsify routing information; and unsolicited commercial e-mail using a third party's Internet address or domain name without permission. Some states require that the unsolicited commercial e-mail must include the sender's name, street address, and e-mail address, along with opt-out instructions (Coalition Against Unsolicited Commercial Email, 1999). The following Table 4 compares the differences between the legislation modes of the U. S. states.

Table 4: Legislation Modes concerning Identity

Criminalization or Requirements		States
Criminalization	The act of sending unsolicited bulk e-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of	Arizona, Arkansas, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee,

	origin or routing information	Texas, Utah, Virginia, Washington, West Virginia, and Wyoming
	The sale, distribution, and possession with intent to sell software that is designed to falsify routing information	Arkansas, Connecticut, Delaware, Illinois, Kansas, Louisiana, Michigan, Nevada, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, and West Virginia
	Unsolicited commercial e-mail using a third party's Internet address or domain name without permission	Arizona, Arkansas, Colorado, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Minnesota, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Texas, Washington, West Virginia, and Wyoming
Requirements	Require that the unsolicited commercial e-mail must include the sender's name, street address, and e-mail address, along with opt-out instructions	Arkansas, Colorado, Indiana, Iowa, Kansas, Maine, Minnesota, Missouri, Nevada, new Mexico, Ohio, Oklahoma, Rhode Island, Tennessee, and Utah

These different provisions within one nation indicate that the law enforcement is confronted with either the jurisdictional gap or overlap, besides possible consistency and coordination.

4. Criminal liability, administrative liability, civil liability, and international cooperation

The prohibition of spam is ensured by liability mechanisms. The liabilities for spam can take the forms of criminal, administrative and civil liabilities. In nature, the criminal liability is the most severe and deterrent one. The administrative and civil liabilities are less deterrent. But deterrence is not the only factor in determining the adoption of liabilities. The most deterrent liability might also be the most costly and thus less efficient in economic sense. Therefore, other liabilities can have comparative advantages. In either case, the international coordination and cooperation are necessary.

In some of the U.S. states, spam has been criminalized by state laws, such as Colorado, Nevada, Pennsylvania, Connecticut, Delaware, Louisiana, North Carolina, and Virginia. In some other jurisdictions without statutes regulating commercial spam, unsolicited e-mail is usually regulated with reference to harassment, stalking, and sexually explicit communication to minors, such as in Hawaii, Wisconsin, and Maryland (Gilbert & Harrison-Watkins, 2001). The Section 4 of 2004 CAN-SPAM Act prohibits using a computer without authorization to send commercial e-mail; falsifying header information in sending commercial e-mail; and registering e-mail accounts with false identifying information, and using those accounts to send commercial e-mail. Under the Act, violations of the provisions above can result in fines and imprisonment of between one and five years depending on the seriousness of the violation and other factors.

In exploring the criminal liability for spam, there are some issues deserving reconsideration.

Firstly, although the overall losses caused by spam are huge, the average loss of a single user by a single message might be very tiny. Every single user might lack the incentive to report and provide evidences to the law enforcement. If they do so, the process might involve more expenses of time, money, and energy than merely being spammed, without

any expected reward. A simple reaction of users against spam might be to ignore it, until they have more sufficient psychological pulse and economic motive to report it.

Secondly, the cost of tracking down spammer is high (Prince, 2004). Although there are cases of harsh criminal sanctions, such as that a Virginian spammer was sentenced to nine years in prison for sending 10 million e-mails each day (Wakefield, 2005), the cases of large damages, such as that another spammer was sued by AOL for 7 million dollars (Ibid), and that a Florida-based spammer, James McCalla was imposed the uncollectible fine of 11 billion dollars for sending over 280 million unsolicited e-mail messages, and an enforceable mechanism of banning him to use the Internet for three years (Arnfield, 2006). Spamhaus estimated that spam would account for 95 percent of all e-mails by mid-2006 (Wakefield, 2004).

Thirdly, the countries adopted different legal approaches, such as opt-in, opt-out, and even no regulation at all. Within each mode, the nature and scope of the regulated messages varies from one country to another. The countries without anti-spam law neither protect the spammed nor prevent the spammer. The users become the potential targets of the spam, while the spammers might emerge in these countries or move to these countries to spam. Every country has the possibility of becoming a safe haven for spammers. This makes it less effective to coordinate internationally.

Fourthly, in addition to the high cost, and the legal and jurisdictional differences, the uncontrollability of the e-mail communications, and the trans-territorial or trans-national distribution of both the spammers and the spammed determine the very low detection and conviction probability. The traditional view supposed a more severe penalty as a more suitable deterrence. But if the probability is near zero, even the highest punishment does not work. All these factors have influence on the effectiveness of criminal liability.

In China, the regulation and punishment of spam are realized through administrative liability. The Article 24 of the Law provides that sending unsolicited e-mail, sending e-mail with false header and labeling, or sending e-mail to recipient who opt-in previously but opt-out subsequently, should be corrected under the order of Ministry of Information Industry or Bureau of Communications Management, and imposed a fine no more than 10,000 RBM Yuan (about 1,000 euros); those who obtained illegal income, should be imposed a fine no more than 30,000 RMB Yuan (about 3,000 euros).

It is also possible to take civil actions against spam senders. First of all, because the ISPs' systems are repeatedly burdened by huge volume mailings, they can incur noteworthy cost. Thus, they have the choice of seeking financial compensation through civil action. Generally, civil laws that apply to damages resulting from wrongful actions or breaches of contract would apply to conventional and online activities equally (Ferguson & Piragoff, 1997).

Another form of civil action can also protect recipients from spamming. Damages are a favorable deterrent against spam. Laws in some of the U.S. states provide statutory damages to individuals and ESPs. These damages vary from 10 dollars per message in Colorado and Iowa to 500 dollars in Rhode Island.

Law enforcement needs the harmonized international actions. There have been a number of international initiatives to deal with the problem of trans-border scams. The Organization for Economic Cooperation and Development adopted new guidelines in June 2003 to promote international cooperation against trans-border fraud and deception. Recent trends in international cooperation have been between industries, organizations and the consumer or citizen, and between industries and government (Ahn, 2004). Important multi-lateral organizations include the Organization for Economic Cooperation and

Development, International Telecommunication Union (ITU), APEC, Internet Corporation for Assigned Names and Numbers (ICANN) and International Consumer Protection and Enforcement Network (ICPEN). In order for the international cooperation to be timely and effective, it should include various different communities (OECD, 2004). In dealing with the problem of spam, the new-styled international cooperation is an urgent call. As of 2005, International Council on Internet Communications was formed to coordinate international efforts to stop spammers (News Target, 2005). Given spam is still in its rapid developing stage, we cannot expect any of such institutions are able to solve the problem in a predictable period.

International action might meet obstacles impossible to overcome. The senders and recipients in opt-in countries and the opt-out countries might first meet with unsolvable vicious cycle. The users of opt-in countries might always feel that they are annoyed by the senders of the opt-out countries. The users of the opt-out countries might feel that they are less informed by the businesses of the opt-in countries. The businesses of the opt-out countries might also feel that they are guilty of spamming users of opt-in countries. The senders of the opt-in countries might feel that they are less competitive in the e-marketing in the global market, and so forth.

Furthermore, we mentioned the different provisions of the subject line. The English-speaking countries will surely require a label in English, such as "ADV", and so forth. Other countries require a label either in their native languages or in English. This brings about little problem within one jurisdiction. The problem is that e-mail advertisements are neither language dependent nor jurisdiction dependent; laws of most countries are, nevertheless, jurisdiction dependent, protecting recipients and preventing senders in one jurisdiction. Neither are the spammers from abroad are well punished, nor are the spammed from abroad well protected. Trans-national spamming is a problem that domestic laws are reluctant to deal with.

Finally, it is less possible to determine whether a message with a specific label is spam according to the domestic laws. If a Chinese sender, fully coincident with Chinese law, sends a message with a label in Chinese character to a user in Japan, who is also a Chinese citizen, he/she might identify this Chinese message as spam according to Japanese law, whether he/she consent to receive such a message or not. Because he/she receives the message in Japan, where only Japanese law applies, he/she can take an action against this Chinese sender on the basis that this message provided the irregular label.

From the above analysis, international cooperation should not only propel unified rules, but also hold spammers liable for trans-border spamming. More than ever, an international anti-spam agreement is necessary.

Concluding remarks

Spammers are motivated by greater benefits from spamming than other kind of direct mailing. The growth of spam despite the increase of efforts suggests that any previous solution cannot work alone. Comprehensive mechanisms must be established to protect the spammed and to discourage the spammer. To balance the liability among the spammer, the spammed, and the intermediaries, criminal sanctions, civil remedies, and international harmonization are all constituents of the effective legal framework.

Acknowledgements

The author would like to thank the anonymous reviewers of *Webology* for their invaluable encouragement and valuable comments on this article.

References

- Ahn, S. (2004, January 22). Background Paper for the OECD Workshop on Spam, OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy.
- Arnfield, R. (2006, January 5). Florida Slaps Spammer with $11 Billion Fine. Retrieved March 15, 2006 from http://www.seeweekly.com/hosting-florida-slaps-spammer-with-11-billion-53252.html
- Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring Spyware Effects. Retrieved March 15, 2006, from http://psi.bth.se/mbo/exploring_spyware_effects-nordsec2004.pdf
- Coalition against Unsolicited Commercial Email (1999, December). *CAUCE News*, 3 (4). Retrieved March 15, 2006, from http://www.cauce.org/node/110
- Cobb, S. (2003). The Economics of Spam. Retrieved March 15, 2006, from http://www.spamhelp.org/articles/economics_of_spam.pdf
- Direct Marketing Association. Executive Summary of International Spam Laws. (n.d.). Retrieved March 15, 2006, from http://www.the-dma.org/antispam/spamlaws.html
- EquIP Technology & CipherTrust. (2004). Spam and Productivity Theft- a Growing Concern for UK PLC. Retrieved March 15, 2006, from http://www.apig.org.uk/equipandciphertrustevidence.doc
- Federal Trade Commission (1998, July). FTC Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, FTC Consumer Alert.
- Federal Trade Commission. (2003, June 15). *National Do-Not-E-mail Report to Congress*, Author.
- Ferguson, P., & Piragoff, D. K. (1997). Internet and Bulk Unsolicited Electronic Mail. Retrieved March 15, 2006, from http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf
- Gartner Consulting. (1999). ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition, Author.
- Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General.
- Gilber, S. & Harrison-Watkins, T. (2001). SPAM: Survey of State and Federal Legislation. Retrieved March 15, 2006, from http://gsulaw.gsu.edu/lawand/papers/su01/gilbert_harrison/
- Goodman, J. T., and Rounthwaite, R. (2004). Stopping Outgoing Spam. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17-24 May, ACM Press, pp. 30-39.
- Goodman, P. S. (2000, December 13). Verizon Online User's E-mail Problems Persist, *Washington Post*, E01.
- Grimes, A. (2003, May 22). Digits: Spam Pays. *The Wall Street Journal*, B3.
- Hansell, S. (2003, July 29). The High, Really High or Incredibly High Cost of Spam. *The New York Times*.
- Hong Kong Information Security Website. (2005, July). Approaches to Cope with Unsolicited Messages. Retrieved March 15, 2006, from http://www.infosec.gov.hk/english/antispam/e-mail/e-mail6.htm
- IDC (2005, February 24). Worldwide Revenue for Antispam Solutions To Reach Over $1.7 Billion in 2008, IDC Reveals. *IDC - Press Release*. Retrieved March 15, 2006, from http://www.idc.com/getdoc.jsp?containerId=prUS00085505
- IMT Strategies. (2001). Raising the Stakes in Permission Marketing. Stanford: Author. Retrieved March 15, 2006, from http://www.imtstrategies.com/download/TI13.01.pdf
- InfoWorld (2003, July). What is the Worst IT Disaster of the Last Year. *InfoWorld*.

- International Telecommunication Union (2004). *Meeting Announcement: ITU WSIS Thematic Meeting on Countering Spam*. Geneva: CICG, July 7-9.
- Kelly, J. S. (2002). A Brief History of Spam. Retrieved March 15, 2006, from http://www-106.ibm.com/developerworks/linux/library/l-spam/l-spam.html
- Khong, W. K (2001, October). The Law and Economics of Junk E-mails (Spam). Retrieved March 15, 2006, from http://www.frg.eur.nl/rile/emle/Theses/Khong.pdf
- Khong, W. K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1 (February), 23-45.
- Korea Information Security Agency (2003). Korea Spam Response Center-Legislation for Anti-Spam Regulations: Mandatory Indication of Advertisement. Retrieved March 15, 2006, from http://www.spamcop.or.kr/eng/m_2.html
- Korea Information Security Agency, Personal Data Dispute Mediation Committee (2003). *Introduction to Act Related to Spam in Korea*, Author.
- Libbenga, J. (2005, July 21). Biggest 419 Bust in History. Retrieved March 15, 2006, from http://www.theregister.co.uk/2005/07/21/scammers_nabbed/
- Living Internet (2005, June 6). E-mail Spam. Retrieved March 15, 2006, from http://www.livinginternet.com/e/et_spam.htm
- Mail Abuse Prevention System (2004). Definition of Spam. Retrieved March 15, 2006, from http://www.mail-abuse.comSpam-def.html
- Midnet Media (2003). Economics of E-mail. Retrieved March 15, 2006, from http://www.midnetmedia.com/BUILD/PDF/MMPG4.pdf
- Moran, J. M. (2002, June 30). Spam King Living High in the Bayou. *The Hartford Courant*.
- News Target (2005, April 28). New International Anti-Spam Council Pledges to Fight Spam around the World. Retrieved March 15, 2006, from http://www.wired.com/news/technology/0,1282,64383,00.html?tw=wn_tophead_5
- Niall, J. (2000). *The E-mail Marketing Dialogue*. Cambridge: Forrester.
- OECD (2003). *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author.
- OECD (2004). *Second OECD Workshop on Spam: Report of the Workshop*, Author.
- PC World (2003, August 29). Sobig May Be Working for Spammers. Retrieved March 15, 2006 from http://www.pcworld.com/news/article/0,aid,112261,00.asp
- Peppers, D. & Rogers, M. (2000). *E-mail Marketing Maximized* . Stanford: Peppers.
- Prince, M. (2004). How to Craft an Effective Anti-Spam Law. June. Retrieved March 15, 2006, from http://www.itu.int/osg/spu/spam/
- Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*, Author.
- Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., and Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.
- Sandiego Media (2005). E-mail Marketing Solution. Retrieved March 15, 2006, from http://www.sandiegomedia.com/cgi-bin/main/co_disp/displ/strfnbr/101/pgname/e-mail_marketing_benefits
- Simon, H. A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. MIT Press.
- Sipior, J. C., Ward, B. T., & Bonner, P. G. (2004, June). Should Spam Be on the Menu? *Communications of the ACM*, 47 (6), 59-63.
- Sorkin, D.E. (2006). Spam Laws. Rretrieved March 15, 2006, from http://www.spamlaws.com
- Taiwan Ministry of Transportation and Communications, The Directorate General of Telecommunications (2005). Questions and Answers on Relevant Topics about Draft Regulations on Unsolicited Commercial E-mail. Retrieved March 15, 2006, from http://www.dgt.gov.tw/chinese/ncc/mail-requlation/ncc-SPAM-Q&A-940215.doc

- TopTenReview (2005). What Makes a Great Internet Filter Software Solution? Retrieved March 15, 2006 from http://internet-filter-review.toptenreviews.com
- Templeton (2003). Origin of the Term "Spam" to Mean Net Abuse. Retrieved March 15, 2006, from http://www.templetons.com/brad/spamterm.html
- Wakefield, J. (2005, April 21). UK Laws Are Failing to Deter Spam. *BBC News*. Retrieved March 15, 2006, from http://news.bbc.co.uk/1/hi/technology/4466053.stm
- World Summit of Information Society (2003). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*, Author.
- Wreden, N. (1999, January 9), Mapping the Frontiers on E-mail Marketing. *Harvard Management Communication Letter*, 6-8.
- Wright, N. D., & Bolfing, C. P. (2001). *Marketing via E-mail: Maximizing its Effectiveness without Resorting to Spam*. James Madison University.
- Xie, T. (2005). Comments on Hong Kong Bill against Unsolicited Electronic Message". November 21, 2005. Retrieved March 15, 2006, from http://www.chinaeclaw.com/News/2005-11-21/4904.html
- Zeller, T., Jr. (2005, February). Law Barring Junk E-mail Allows a Flood Instead. *The New York Times*, A1.

Footnote

1. See Living Internet (2005) for details of the message.
2. The invisible hand is a metaphor created by Adam Smith to illustrate the principle of "enlightened self interest".
3. See Australia SPAM Act 2003; China Management Measures on Internet E-mail Services 2005, Article 13 (2) and (3), and Article 14; European Directive 2002/58/EC; and the United Kingdom Privacy and Electronic Communications (EC Directive) Regulations 2003.
4. See Canada Personal Information Protection and Electronic Documents Act (2000, c. 5); Japan Specified Commercial Transactions Law for Appropriate Transmission of Specified E-mails 2002; Korea Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 (revised December 18, 2002); Singapore Proposed Legislation Framework on Controlling Unsolicited E-mail (Singapore Information Development Agency and Singapore Department of Justice); Taiwan Draft Regulations on Unsolicited Commercial E-mail; the United States CAN-SPAM Act (Controlling the Assault of Non-solicited Pornography and Marketing Act 2003) 2003.

Bibliographic information of this paper for citing:

Li, X. (2006). "E-marketing, Unsolicited Commercial E-mail, and Legal Solutions." *Webology*, **3**(1), Article 23. Available at: http://www.webology.org/2006/v3n1/a23.html

---

This article has been cited by other articles.
