Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

22-Jan-2004

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP(2003)10/FINAL
Unclassified

BACKGROUND PAPER FOR THE OECD WORKSHOP ON SPAM

JT00157096

English - Or. English

FOREWORD

This paper was presented to the Working Party on Telecommunications and Information Services Policy (TISP), the Working Party on Information Security and Privacy (WPISP) and the Committee on Consumer Policy during their meetings in 2003. It was declassified by the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy in January 2004.

The report was prepared by Mr. Sung-il Ahn of the OECD's Directorate for Science, Technology and Industry. It is published on the responsibility of the Secretary-General of the OECD.

BACKGROUND PAPER FOR THE OECD WORKSHOP ON SPAM

TABLE OF CONTENTS

INTRODUCTION

The major role of Internet and e-mail

As the number of Internet users increase, the Internet is gradually becoming an integral part of everyday life. Usage is expected to continue to grow. The number of Internet users in the OECD area was 213 million in 2001[1] and worldwide over 591 million in 2002.[2] Expected worldwide usage is forecast to reach between 709.1 million to 945 million users by 2004.[3]

Many market analysts have viewed e-mail as one of the "killer applications" for the growth of the Internet. E-mail is quickly joining the telephone as an essential communication tool in people's commercial and social lives. E-mail has become a powerful medium, not only for idea and information exchange, but for e-commerce including direct marketing. With its role as a quick and relatively inexpensive form of communication, e-mail has developed as one of the primary communication mechanisms for personal and business use.

The International Data Corporation (IDC) estimates that there are about 700 million electronic mailboxes in the world and that the number will grow to 1.2 billion in 2005.[4] IDC estimates that e-mail volume will continue to expand rapidly. Estimates suggest that some 31 billion messages were sent over the Internet in 2002, and that the number will reach or surpass 60 billion in 2006.[5]

Growth in spam

Along with the growth of the Internet and e-mail, there has been a dramatic growth in bulk unsolicited electronic messages (commonly referred to as spam) over the last several years. [6] Spam can originate from any geographic location across the globe because Internet access is available in over 200 countries. The ease with which spammers can change the originating server for their messages means that even if the domestic e-marketing culture discourages spam, or legal restrictions are in place, spam messages can easily be sent from other locations. Despite the increasing deployment of anti-spam services and technologies, the number of spam messages continues to increase rapidly.

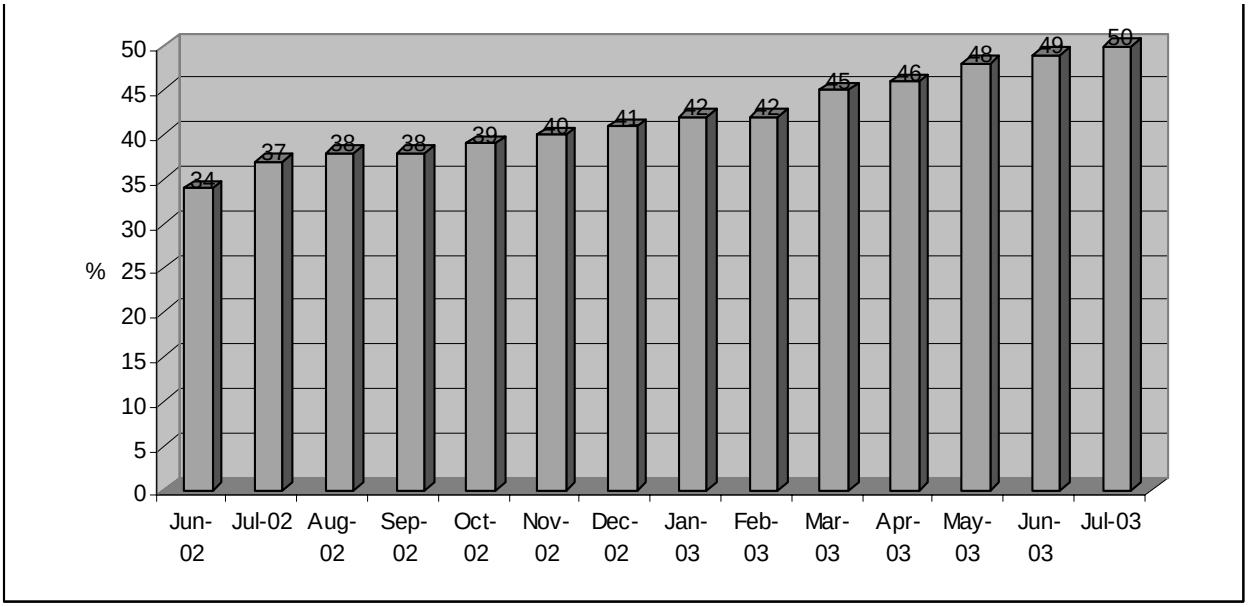
The following statistics in Figure 1 show how fast spam has grown recently. According to Brightmail, an anti-spam software company, as of July 2003, unsolicited bulk mail volumes accounted for 50% of all e-mail traffic on the Internet, up from just 8% of traffic in mid-2001. Another anti-spam solution company, MessageLabs, found that 55% of the e-mails it scanned in May 2003 were spam. The Radicati Group estimates that 4.9 trillion spam e-mails will be sent in 2003.[7] The growth rate is expected to increase in the future.

Spam is a problem not only for personal e-mail accounts, but for corporate accounts. In particular, America Online (AOL), an Internet service provider (ISP), blocked 2.37 billion spam messages per day in April 2003. This represents increased costs and security risks to businesses and consumers alike.

Even though some major e-mail service providers and research companies provide their data associated with spam, more data on the problems caused by spam, the rate of growth in spam, and the success of various proposed solutions would be useful to diagnose the current situation more precisely for

formulating anti-spam policies. Further reflection is required as to which appropriate bodies could play a role in collecting data on spam.

Figure 1. **Percentages of total e-mail identified as spam according to Brightmail**



Source: Brightmail (2003), "Spam Statistics", www.brightmail.com/spamstats.html, accessed 8 December 2003.

Detrimental effects of spam on consumer trust

Consumer trust is key for the growth and success of e-commerce. In order for the Internet to maintain and increase commercial growth, users must have confidence in the security and usability of this electronic medium. The significant increase of spam threatens to erode consumer confidence online, which in turn has a negative effect on the growth of the digital economy. The intrusiveness of spam, and the fact that much spam is also linked to fraudulent or deceptive or pornographic commercial activities has harmed the development of e-commerce by reducing consumer trust and diminishing the credibility of e-mail marketing.

Purpose and scope of this paper

This paper has been prepared as background information for participants to the OECD Spam Workshop to be held in Brussels on 2-3 February 2004. It contains an initial survey of the problems related to and caused by spam. It focuses on identifying the characteristics of spam, the reasons why spam is increasing and several of the problems raised by spam. These problems include the costs of spam, its impact on communication infrastructures and markets, breaches of privacy and theft of corporate information, spam content, network security and consumer protection issues. The paper also aims to provide a survey of member country initiatives in the area of spam to facilitate an exchange of information as to the impact of different solutions being implemented. Finally, this paper aims to provide a basis for further discussion and information exchange among member countries to counter spam at national and international levels.

OVERVIEW OF SPAM

What is spam?

The difficulty of defining spam

Although a definition of "spam" would be useful, there does not appear to be a widely agreed and workable definition at present. A comprehensive definition might need to incorporate a diverse set of elements related to commercial behaviour, recipient psychology, the broader legal context, economic considerations, and technical issues. To complicate the matter further, the word "spam" itself is not directly related to the topic.[8] Finally, of course, the spam phenomenon is perceived in different ways in different countries. Nonetheless, a number of countries have adopted general working definitions. Examples of the approaches taken in France, Australia, and the European Commission are described below. From these definitions and other discussions of spam, a number of characteristics of spam can be identified.

In France, the *Commission Nationale de l'Informatique et des Libertés* (National Data Processing and Liberties Commission) refers to "spamming" or "spam" as the practice of sending unsolicited e-mails, in large numbers, and in some cases repeatedly, to individuals with whom the sender has no previous contact, and whose e-mail address was harvested improperly.

According to a 2001 European Commission report, "Unsolicited Commercial Communications and Data Protection", *"Spam is generally understood to mean the repeated mass mailing of unsolicited commercial messages by a sender who disguises or forges his identity."* Thus, while it has in common with other forms of commercial communication the fact that it is unsolicited, it differs from them by its massive, repetitive and unfair nature. In short, all spam is by definition unsolicited commercial communication but not all unsolicited commercial communication is spam."[9]

Australia's 2003 "Final Report of the NOIE (National Office for the Information Economy) Review of the Spam Problem and How It Can Be Countered" states that spam is *"the term now generally used to refer to unsolicited electronic messages, usually transmitted to a large number of recipients."* They usually, but not necessarily, have a commercial focus, promoting or selling products or services; and they share one or more of the following characteristics:

- They are sent in an untargeted and indiscriminate manner, often by automated means.
- They include or promote illegal or offensive content.
- Their purpose is fraudulent or otherwise deceptive.
- They collect or use personal information in breach of the Privacy Act 1988 National Privacy Principles (NPPs).
- They are sent in a manner that disguises the originator.
- They do not offer a valid and functional address to which recipients may send messages opting out of receiving further unsolicited messages."[10]

Characteristics of spam

Extrapolating from the discussions above and elsewhere, the following characteristics[11] can be associated with spam:

- **Electronic messages:** spam messages are sent electronically. While e-mail is by far the most significant channel for spam, other delivery channels include short message services (SMS) or SM-Caster (messenger spam).
- **Bulk**: spam messages are typically sent in bulk, but can be sent in smaller parcels via "free" e-mail accounts.
- **Unsolicited**: spam is sent without the recipient's request or consent. Determining whether a message is unsolicited may be difficult where there is a pre-existing relationship between the sender and the recipient.
- **Commercial**: typically spam has a commercial purpose: the promotion or sale of a product or service. However, some non-commercial messages may also be considered spam, for example unsolicited bulk messages with a political theme or that contain a virus.
- **Uses addresses collected or sold without the owner's consent**: Spammers often use e-mail addresses that have been collected without the owner's explicit consent. For example, many spammers use address lists electronically harvested from public sources, such as Web pages or newsgroups.
- **Unwanted**: spam is usually considered to be unwanted or even useless by its recipients.
- **Untargeted or indiscriminate:** typically spam is sent in an indiscriminate manner, without any knowledge about the recipient other than the e-mail address.
- **Repetitive**: many spam messages are repetitive, either exact duplicates of prior messages (or containing very slight variations).
- **Contain illegal or offensive content:** spam is frequently a vehicle for fraudulent or deceptive content. Other spam includes adult or offensive content, which may be illegal in some countries.
- **Unstoppable:** spam recipients are typically unable to stop the reception of the messages. This is because unsubscribe links typically do not work.
- **Anonymous or disguised**: spam messages are often sent in a manner that disguises the originator by using a false address or header information. Spammers frequently use unauthorised third-party e-mail servers.

For purposes of this paper, the characteristics above may be classified as either primary or secondary. The *primary* characteristics include unsolicited electronic commercial messages, sent in bulk. Many would consider a message containing these primary characteristics to be spam (see Table 1). The remaining characteristics identified above may be described as *secondary* characteristics which are frequently associated with spam, but not perhaps as necessary. Regulation in some OECD countries applies to messages that include a mix of the characteristics identified as primary and secondary in the table below.

Table 1. **Primary and secondary characteristics of spam**

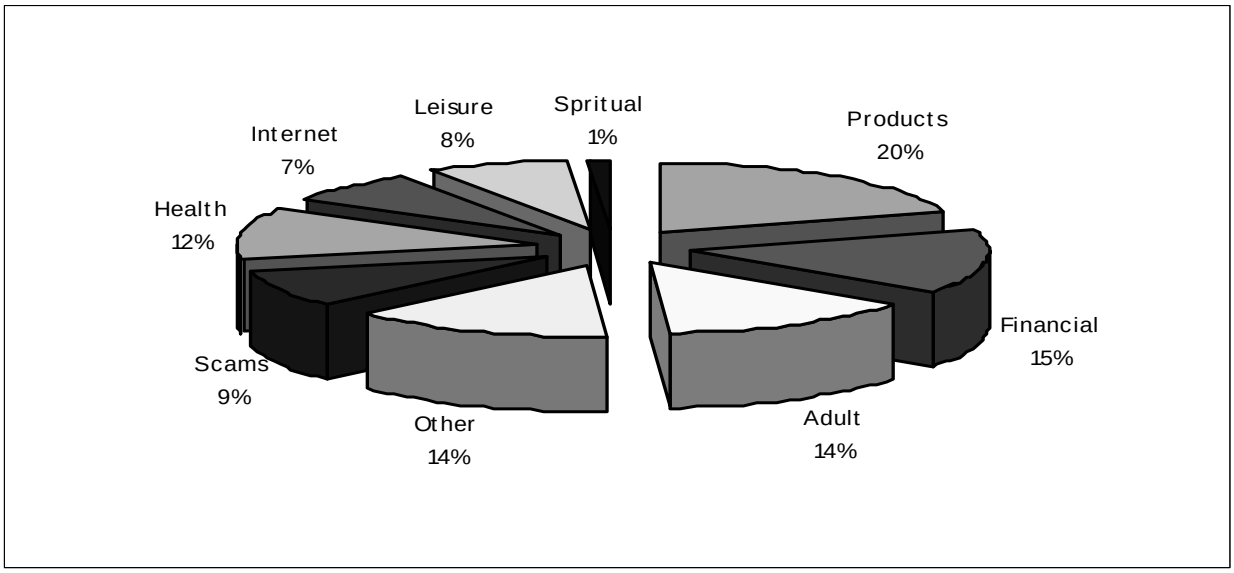
Primary characteristics	Secondary characteristics
Electronic message	Uses addresses collected without prior consent or knowledge
Sent in bulk	Unwanted
Unsolicited	Repetitive
Commercial	Untargeted and indiscriminate
	Unstoppable
	Anonymous and/or disguised
	Illegal or offensive content
	Deceptive or fraudulent content

Source: OECD Secretariat.

Categories of spam content

The content of spam messages ranges enormously, from advertisements for goods and services to pornographic material, to information on illegal copies of software, to fraudulent advertisements and/or fraudulent attempts to solicit money. To illustrate the different range of spam messages, Figure 2 shows a measure of the distribution of spam category data for a given period of time.

Figure 2. **Spam category data**



Source: Brightmail's Prove Network (2003), "The State of Spam - Impact and Solutions", Brightmail, July, www.brightmail.com/press/state_of_spam.pdf, accessed 9 January 2004.

Economics of spam

Spam has become one of the more controversial issues affecting e-commerce. What incentive is there for spammers to send electronic messages?

Tool for direct marketing

The development of sophisticated databases has made telemarketing and e-marketing increasingly popular as a direct marketing strategy. The forms of direct marketing include postal mail, telephone, fax, automatic calling machines and e-mail. Direct marketing is viewed by companies as an important tool to approach, inform and retain customers, as well as provide customer relationship services. Electronic messages including e-mail provide a cheap and easy way to contact a large group of customers. E-mail has also become one of the most cost-efficient ways to provide customer support and assistance. The recognition that the Internet has decreased customer-switching costs in many cases has highlighted the importance of customer relationship management and permission marketing. However, these benefits have been put at risk by the continued flood of spam, by reducing the customer confidence in, and effectiveness of, e-mail marketing.

Low or transferred costs

E-mail may be the cheapest vehicle for direct marketing; costs do not vary according to distance and repeated e-mails have very low additional costs. The very low marginal cost of sending bulk e-mail to individual addresses means that if only one of the addressees becomes a commercial customer, the costs of the particular direct marketing approach can probably be recovered. Therefore, e-mail can be an ideal, cost-effective way to build relationships with customers. This also explains why spam is growing at such an alarming rate. Because the costs of sending spam are so low, spammers can make a profit despite extremely low response rates. The more e-mails a spammer can send, the greater the profit, while costs remains nearly constant.

In a 2002 survey on the commercial use of e-mail, it was estimated that the cost to send a single e-mail averages USD 0.05 with a low value of USD 0.01.[12] Other research has suggested that it costs 0.00032 cents to obtain one e-mail address.[13] However, because of the range of methods used to obtain e-mail addresses, it is difficult to provide accurate data on costs at this stage. It is certain, however, that these costs are extremely low.

A significant difference between other direct marketing forms of unsolicited advertising and spam is that spam shifts the cost of advertising to the entities that receive and deliver the e-mail such as ISPs, enterprises, and consumers. With other forms of unsolicited advertising, the advertiser pays to send advertisements and the consumer is simply inconvenienced or annoyed by receiving them. To produce and distribute regular mail, layout work, paper costs, folding, and stamping are necessary, whereas telephone marketing requires a large number of staff. On the other hand, one who sends bulk e-mail often pays very little of the actual distribution costs and it appears that this low cost enables indiscriminate use of the medium. The sheer volume of messages imposes significant costs related to blocking or eliminating large numbers of unwanted messages on receiving ISPs, corporate systems and consumers.

With low costs, low response rates will show a profit through spam nonetheless. According to a survey conducted by Mailshell in March of 2003, more than 8% of the 1 118 respondents admitted that they have actually purchased a product promoted via spam. [14] A study by the Wall Street Journal in 2002[15] showed that a return rate as low as 0.001% can be profitable when using e-mail. In one case cited, a mailing of 3.5 million messages resulted in 81 sales in the first week, a rate of 0.0023%. Each sale was worth USD 19 to the marketing company, resulting in USD 1 500 in the first week. The cost to send the messages was minimal, probably less than USD 100 per million messages. The study estimated that by the time the marketing company had reached all of the 100 million addresses it had on file, it would probably have pocketed more than USD 25 000 on the project.

Why is spam proliferating?

In addition to the economic factors described above, other factors may account for the increasing volume of spam. One such factor is the sophistication of the current tactics for obtaining e-mail addresses. Another factor is the difficulty of identifying spammers in order to hold them accountable for their practices.

E-mail address gathering and sending technology

A spammer can obtain e-mail addresses from the following sources:

1) Customers or prospective customers who supply their e-mail address to the spammer themselves.

2) Third parties who obtained the addresses directly from the individuals and sell them to the spammer.

3) Public spaces such as Web pages, directories or newsgroups on which the spammers harvest the addresses using spamware.

4) Third parties who used spamware to harvest individuals' addresses from public spaces and sell them to the spammer.

5) In some cases there are also formulas (automated guesses related to first or last name) used against a specified domain.

Among these sources, the third and fourth methods are the most common.[16] Only the first method might result in a recipient being aware that their e-mail address was being used for spam. To obtain e-mail addresses, spamware tools automatically navigate Web sites and public spaces such as Usenet or chat rooms, using a list of URLs either specified in advance, created by means of keywords entered into search engines or recursively grabbed from Web pages in a search-engine fashion. They then collect all the e-mail addresses found on those spaces. They also distribute e-mail to lists created to circumvent filters put in place by the ISPs.

Some spamware programs use other techniques to gather e-mail addresses. One is the random e-mail address generator. A bulk e-mailer floods a particular domain name by using a program that generates millions of possible Web addresses, such as aa@cdt.org, ab@cdt.org, and so on. This "brute force attack" attempts to send e-mails to every possible combination of letters that could form an e-mail address. The more elegant "dictionary attack" builds address lists through computer-generated alphabetic permutations combined with address suffixes or creates addresses by using common surnames and first initials (*i.e.* names are taken sequentially, for example bob@msn.com, abob@msn.com, bbob@msn.com, cbob@msn.com, etc.).

Major ISPs and corporate networks which handle a large volume of e-mail traffic on their servers everyday are highly vulnerable to the dictionary attack, because spammers often conduct the attacks undetected, hidden in normal traffic. Spammers sometimes use software which opens connections to the other mail servers and automatically submits millions of random addresses, such as "anne@hotmail.com", "michael@hotmail.com", recording which addresses succeed. These are then added automatically to the spammer's list.[17] Spammers mainly target ISPs, but spammers also spam enterprises so as to reach the corporate inboxes of millions of e-mail users. Though the purpose of such attacks is not to alter the service of the attacked machines, its effect on ISPs or enterprises is similar to a denial of service (DoS) attack, wherein legitimate use of the ISP's services is denied by massive illegitimate traffic.

Some spammers gather lists of working e-mail addresses not for spamming, but for resale in bulk to other spammers worldwide.[18] In fact, a fair number of spammers are not interested in selling goods and services. Instead, they make money selling e-mail addresses to other spammers.

The difficulty of identifying spammers

Identifying spammers is difficult. A number of methods are used by spammers to hide their identities. Source addresses are randomised so that they are not easily identified. Spamware programs automatically generate false headers and return address information. False headers allow spammers to ignore recipient requests to be removed from e-mail lists and to obscure their identities by making themselves untraceable. Other spammers scan the Internet for open relays in foreign countries for their messages not to be traced. According to Spamhaus, direct spam sources "account for some 50% of spam received by Internet mail relays worldwide, the other 50% comes via third-party exploits such as open proxies and open relays."[19]

Some spammers open free e-mail accounts and abandon them before they're caught. Spammers also write programs that load in multiple accounts so when one account is terminated, another automatically kicks in. Quite a few spammers simply move on to another ISP when their accounts are terminated for spamming with another ISP. However, others pretend to their ISP providers to be small ISPs themselves, claiming that the spam is coming from non-existent customers.[20] Spammers can send out hundreds of thousands of messages, each with customised content and source addresses, and then quickly log out.[21] "Spoofing" addresses is also used by spammers. This involves using false information as to the name of the sender. This can be either false information or in some cases using names of other commercial entities that are not involved with the spam operation.

According to Spamhaus, which operates a Register of Known Spam Operations (ROKSO), 90% of all spam received by Internet users in North America and Europe is sent by a core group of only 180+ individuals, almost all of whom are listed in the ROKSO database. These professional, chronic spammers are loosely grouped into gangs ("spam gangs") and move from network to network seeking out ISPs known for not enforcing anti-spam policies.

Spam in the wireless world

With the continued adoption of wireless communications worldwide, the development of third generation wireless networks and the growing use of mobile messaging for unwanted commercial messages, there is a growing need for anti-spam protection in the wireless environment. As mobile phones or mobile devices such as personal data assistants (PDAs) continue to spread, spammers will be increasingly attracted to spamming wireless users. While text messaging has yet to catch on in some member countries (*e.g.* United States), it has been a popular feature of cell-phone service for years in others (*e.g.* Finland, Japan, Korea, United Kingdom), where wireless spam is already a problem.

In the case of the United Kingdom, SMS messaging is growing more and more popular. Over 6 billion text messages were sent in 2000, and over 12 billion in 2001. A typical type of SMS spam asks recipients to urgently call a Premium Rate Service number (PRS). Calls to PRS numbers cost up to GBP 1.50 per minute in the United Kingdom. These numbers may be linked to information 'services' which provide nothing of value and/or have been set up purely as a scam. Another typical SMS scam message reads, "URGENT please call certain number," where the number is a PRS. Other types of SMS spam involve third parties promoting their products and services to other companies' customers. There have been cases where the caller will hear only a recorded engaged tone for which they will be charged. This is used to encourage people to redial the number for further charges. Related schemes are operated in the online context, causing a PRS connection to be generated via a computer dial-in through a spoofed link.

The advent of text messaging has made mobile phones particularly vulnerable to dictionary-type attacks by spammers using phone numbers. In addition, as wireless devices become more multifunctional (by combining phone, camera, MP3 player, etc.) protection from viruses spread by spam will become even more critical.

Wireless carriers also confront customer churn and costly refunds for unwanted wireless spam. Under the wireless messaging pricing models in which wireless users or recipients must pay for message and content within a message, customers and mobile service providers bear the cost of spam. For example, in Japan, a wireless service provider, DoCoMo refunds their customers for each spam message received as DoCoMo charges for incoming messages. The initial open nature of DoCoMo's address system aggravated problems for users in 2001. DoCoMo recommended that users change their mail addresses and over 90% of them had changed their addresses by the end of January 2002. With unwanted messages flooding wireless devices, some end-users may consider wireless devices impracticable as communication tools.

Various anti-spam efforts have been made by wireless carriers, associated organisations and users. In the United States, wireless carriers have set up systems to discourage spam by blocking bulk messages and keeping their customer lists private. In January 2001, the Mobile Marketing Association (MMA) established privacy guidelines for its members based on the premise that wireless push advertising should only be sent to customers who have asked for it. The MMA also declared that wireless spam would serve neither the needs of consumers nor the wireless industry, and that "confirmed opt-in" should become the *de facto* standard for wireless push advertising.[22]

In Japan, DoCoMo has tried to prevent advertisers from creating accurate target lists by blocking the spammers' ability to send ads to large numbers of DoCoMo e-mail addresses. It started using alpha-numeric mail addresses as defaults instead of phone numbers, and providing 400 packets per month free of charge as a buffer, as users are charged for receiving e-mails as well as sending them. In addition, users have blocked e-mails from unspecified addresses and changed their e-mail addresses.

In the United Kingdom, three of Britain's mobile phone companies, BT Cellnet, Vodafone and Orange, adopted a code of practice in March 2001 that limits the sending of unsolicited text messages to mobile phones. The code, drawn up by Wireless Marketing Association (WMA), declares that wireless marketing should only be sent to mobile users if they first grant permission for it to be sent. On the other hand, the UK government runs a scheme called Telephone Preference Service (TPS), through which customers may register their mobile number. It is illegal to make a direct marketing call or to send a marketing SMS to any number on the TPS (now partially overtaken by new opt-in rights for individuals). Customers can also report suspected Premium Rate SMS scam messages to the Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS). Customers may also complain about SMS spam to the Information Commissioner.

On 19 October 2003 the Ministry of Information and Communication (MIC) in Korea announced that it would introduce opt-in for mobile phone service. Opt-in will be implemented via usage agreements between mobile service providers and information service providers. MIC also prohibits sending advertisement messages during certain time periods, for example from 21.00 to 8.00, even for opt-in customers.

WHAT ARE THE PROBLEMS ASSOCIATED WITH SPAM?

Spam is becoming increasingly unpopular among Internet users. A 2002 Harris Interactive survey of US adults suggests that 80% are "very annoyed" by spam, compared with only 49% who responded similarly two-and-a-half years earlier. An estimated 74% are proponents of making spam illegal, while only 12% are opposed to banning it.[23] The sections below outline a number of the reasons that spam has become such a problem.

Costs of spam

Spam imposes costs on all Internet users. These costs have been increasing with the growth in the number of spam messages infiltrating the Internet daily. Certainly spam is a nuisance and the degree to which it is a nuisance has also increased with the growth in spam. More importantly, however, spam uses scarce resources of users and service providers without compensation or approval. Spam consumes network and computing resources, e-mail administrator and helpdesk personnel time, and reduces worker productivity.

It is difficult to calculate the total costs of spam at the global level, though estimates suggest the costs are high. For example, a European Union (EU) study estimates that the worldwide cost to Internet subscribers of spam is in the vicinity of EUR 10 billion a year.[24] The same study estimates that if people receive six spam messages a day, two hours are wasted each year deleting spam (assuming it takes 3-4 seconds to determine the nature of a message and delete it.).[25] A survey of 1 000 consumers conducted by InsightExpress suggests that 65% spent more than 10 minutes each day dealing with spam, and 24% reported dealing with it for more than 20 minutes per day.[26]

Costs for individual users

Consumers waste time deleting repeated unsolicited commercial messages. The costs for consumers can also include additional communications charges from ISPs or telephone companies (or both) as well as additional data storage charges. Likewise, costs incurred by ISPs in dealing with spam tend to be passed on to consumers.

Costs for companies

Companies also have concerns about the significant costs of spam, which threaten the business environment in multiple ways. Using techniques that harvest e-mail addresses on the Internet, spammers have databases of addresses taken from corporate Web sites. Furthermore, the increase in spam attacks on companies introduces serious threats.

Even though the costs for companies can vary according to the methodology used, they may be estimated by looking into several studies. Brightmail estimates the annual costs of spam to a company by assuming that 10% of total e-mail is spam and each employee spends 30 seconds per day deleting spam. Based on these assumptions, the estimated annual cost of spam to a 10 000-person company is

USD 675 000.[27] A June 2003 report from the Radicati Group predicts that e-mail spam will cost companies USD 20.5 billion in 2003, and nearly ten times that amount, USD 198 billion, by 2007.[28]

Ferris Research, Inc. has also estimated that unwanted commercial e-mail cost US corporations USD 8.9 billion in 2002. Ferris computed the cost of spam by calculating its cost effects in three areas: loss of worker productivity; consumption of bandwidth and other technical resources; and use of technical support time. The estimate was equivalent to about USD 10 per user per month.[29] Ferris also predicted that spam will cost US organisations more than USD 10 billion in 2003. In Europe, Ferris estimated the cost of spam at USD 2.5 billion.[30]

The costs of spam to companies can be categorised as follows. First, there is the productivity loss from employees dealing with spam. Second, there are additional costs for network and computing resources. Third, there are additional human resources and financial burdens for deploying technical tools to deal with spam. A fourth category is the security risks due to spam attacks such as dictionary attacks and e-mail-borne viruses and worms. Finally there is potential legal liability.

In terms of reducing employee productivity, the costs include the time spent by employees checking their mail and regularly deleting unwanted advertising messages they receive every day. It is estimated that the cost of time spent in opening and reading spam in the workplace averages AUD 960 (approximately USD 620) per employee each year according to a report by the Australian National Office for the Information Economy.[31] This does not include bandwidth and network costs, and downtime attributable to spam overload.

The network and computing resources to deal with spam messages may be quite high. Spam may require filtering resources, may slow down company networks by increasing the traffic load and will have an impact on the enterprise's computer storage space and bandwidth. Spam consumes e-mail administrator and helpdesk personnel time and increases financial costs for deploying anti-spam technology and operating filtering systems.

Large spam attacks, such as a "directory attack" can paralyse or shut down the company's networks. E-mail-borne viruses and worms pose a serious threat to company networks as well. Some have raised the issue of potential legal liability for companies where they are unable to protect employees from exposure to obscene material in the workplace (*e.g.* porn via spam).[32]

Spam also has a cost for legitimate e-mail marketers. As consumers grow frustrated by spam messages and filters are more widely used, messages from legitimate marketers may also be deleted together with spam. These may include transactional messages or simply provide product or service information. As a result, legitimate e-mail marketers may lose both existing customers and the opportunity to obtain new customers.

Anti-spam measures may impose unintended costs on businesses and consumers by blocking of legitimate messages. As companies and ISPs deploy filtering and blacklisting mechanisms, the incidence of "false positives" increases exponentially. Legitimate business messages which are erroneously filtered out as spam are blocked from reaching their intended recipients, who often do not know their ISP or company has blocked the message. This is occurring with increasing frequency to commercial messages which have been opted-in.

Cost to ISPs and e-mail service providers

ISPs and e-mail service providers (ESPs) also incur many of the costs incurred by companies. These costs include network bandwidth, data storage, staff time, phone-line availability, processing costs incurred

accommodating and routing excess incoming mail, investments in filtering technology, and legal fees incurred fighting spammers in court. In addition, ISPs incur other costs since they have to respond to the growth in spam more rapidly, because the increased volume of e-mail can significantly slow Internet speeds, overload e-mail servers, and even threaten their business itself. ISPs and ESPs require adequate staff resources to deal with spam at the technical level and to respond to complaints received from subscribers. Spam filters put in place by ISPs may erroneously block no-spam messages, resulting in inconveniences to their customers who may switch providers. On the whole, the amount of time and money spent dealing with spam by ISPs and ESPs on filtering, bandwidth and customer service is much greater than the amount seen in other companies.

According to Ferris Research, the spam costs of US and European service providers are estimated at USD 500 million. Other research indicates that the costs to ISPs are 10% of the overhead cost of providing Internet access, which is included in the monthly charges to consumers.[33]

Problems related to privacy

The practice of spamming, and in particular the collection and sale of e-mail-addresses, raises a number of concerns about privacy protection under the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("Privacy Guidelines"). Spamming practices may also violate existing international privacy regulations and national privacy laws. They may especially raise concerns if personal information is misused, causing harmful consequences.

One of the main privacy problems consumers face with respect to spamming is that it causes significant unwanted intrusions into their lives: people receive spam that they simply do not want. Moreover, the collection of e-mail addresses is frequently made without users' knowledge, often with no specification, or an inaccurate specification, of the purpose and without users' consent. These problems are exacerbated when spam is sent indiscriminately. For example, some spammers harvest e-mail-addresses from Web sites, newsgroups and other publicly available sources on the Internet. Other spammers use "dictionary attacks" to send spam. Finally, some spammers even obtain e-mail addresses by hacking into private databases. Additional surveillance over the private lives of users can occur through the introduction of Web beacons and/or spyware on users' computers without their knowledge.

Problems related to spam content

Fraud and deception

Fraudulent or deceptive spam can take a number of forms. According to a US Federal Trade Commission (FTC) report, "False Claims in Spam", released on 30 April 2003, 66% of spam messages are fraudulent in their "from" and/or "subject" lines, or in the message itself.[34] Spammers disguise the origin of their messages because spammers *i)* know their messages are being blocked or filtered; and *ii)* aim to entice individuals to open their messages. A common trick that spammers use is to forge the headers of messages. Spammers often use the relay function in mail servers managed by others.[35] These kinds of problems include false "from" and "reply-to" addresses, false routing information, deceptive subject lines, and fraudulent removal representations. The FTC recently filed a case against a spammer on the basis of deceptive use of the "subject" line, unfair use of a false "from" line and deceptive use of the removal request at the end of a spam message.[36]

It is also commonplace for spam to include deceptive or misleading representations in the body of the message. One popular type of scam is the get-rich-quick scheme, *e.g.* the "Nigerian scam",[37] where the message originator wants to share million of dollars with the message recipient, but usually needs a down

payment in advance. The US Secret Service has designated this type of spam scam as an "epidemic" and claims that losses amount to hundreds of millions of dollars annually.[38] Some scam messages promote pyramid and bogus no-risk investment schemes. Others types of misleading spam advertise "miracle" diets and health products, credit card or credit improvement offers, attractive travel packages and/or business opportunities. There are also various kinds of illicit or illegal spam messages including those that promote prostitution, illegal online gambling services, drugs or weapons sales, and so forth.[39]

Pornography

Spam messages containing pornographic photographs, and promoting adult entertainment products and services[40] are not appropriate for children. Since many spammers do not target specific recipients, young children are likely to be inadvertently exposed to pornographic or offensive messages.

Security implications

Spam can clog computer networks and temporarily paralyse or even permanently damage personal computers when used to spread computer viruses or worms. Large volumes of spam can interfere with critical computer infrastructures and endanger public safety. Spam may also be used maliciously as a Denial of Service (DoS) attack.

Some spam also contains destructive viruses and worms. Virus writers typically write programs that download users' address books and propagate viruses by sending to all users in an address book from a *bona fide* user. By doing this, the virus writers avoid anti-spam filters. Some estimate that 90% of viruses are passed through e-mail. 51% of corporations have had a virus disaster, and computer worms like Klez and Code Red have become prevalent and problematic as well.[41] The experience of spam linked with viruses has led to greater mistrust of e-mail as a secure communication mechanism.

In addition to viruses or worms, files such as Web beacons and spyware can be downloaded with the content of e-mail messages. Spammers also exploit security weaknesses inherent in e-mail transfer technology such as open relays and open proxies. According to MessageLabs, more than 60% of the spam it traps each month is sent via open proxies.[42] Open relays have been identified as a significant enabler of spam and spammers sometimes make unauthorised intrusions to open a closed relay. Some ISPs have refused to accept communications traffic from improperly configured servers or even from countries where a large number of facilities can be used for relaying inappropriate communications.

The linkages between spammers and writers of malicious code seem to be increasing. Spammers are using virus-writing techniques to get their messages through filters. Virus writers also have made use of spammers' mass-mailing techniques for the purpose of attacking computer systems. A recent example is the virus known as "Webber," which was discovered in July 2003. It carried the subject line "Re: Your credit application." Users who opened the attachment downloaded a malicious program that turned a PC into an open relay server, which allows a third party to send or receive e-mail remotely.

Another and more serious case is the "Sobig.E" virus which grabs e-mail addresses from several different locations on a PC, including the Windows address book. Sobig.E then tries to send a copy of itself to each address, using one of the stolen addresses to forge the source of the message. According to MessageLabs, Sobig.E is a spammers' virus designed to harvest legitimate e-mail addresses from users' computers. Using such viruses, spammers can abuse users' address books to send out large amounts of spam messages.

Other security issues are raised by the use of spam to lure unsuspecting users to Web pages where spying software is secretly downloaded. Spyware monitors a user's activity on the Internet and transmits that information to someone else. It may also gather information about e-mail addresses, passwords, and credit-card numbers.

Identity theft

Identity theft is on the rise, threatening e-commerce by eroding consumer trust. Every e-mail contains information regarding its origin, but current technology does not guarantee that the information on the header is correct. If spammers discover that all e-mail from a particular company is allowed through spam filters because the company is on a "white list", spammers can make their e-mails look like they originate from that source. Spammers usually use some other business's IP address or conceal their own identity by using stolen or falsely labelled company identities.[43] Others alter the header to falsify the sender or create an open relay through unsecured servers.

Corporate identity theft can damage a company's brand worldwide. Corporations that are victims of identity theft have to spend significant time and resources recovering their lost image. Moreover, ISP blacklists often include the domain names of these victims of domain identity theft. As a consequence, subscribers to these blacklists can no longer receive e-mail from legitimate enterprises. Nowadays, domain names play an important role in a company brand. So theft of these names for spamming has damaged a number of companies and is expected to increase.

Individuals as well as companies can be victims of identity theft. Many spammers send their messages by using someone else's account without permission, because spamming is an offence or is forbidden by their ISPs. ISPs operating under an industry code of conduct or practice have the power to terminate accounts that are used to send spam.

Reduced consumer confidence

Beyond the costs borne by ISPs and end-users, a major problem of spam is that it creates distrust among Internet users in the digital economy which could have an adverse impact on the development of e-commerce. Spam can lead to consumer reluctance to participate in the Internet, *i.e.* online forums and Usenet groups, or may lead to their removing their e-mail addresses from business and home pages for fear of having their addresses harvested and added to mailing lists. This may prove to be a threat to the usefulness of e-mail, the most successful tool of the Internet.

For a number of years the OECD has been working to build consumer trust and confidence online. In 1999 OECD member countries adopted *Guidelines on Consumer Protection in the Context of Electronic Commerce*. Recognising the importance of fair business and marketing practices to consumer confidence, the *Guidelines* contain provisions related to spam, providing in particular that:

1) Businesses should develop and implement effective and easy-to use procedures that allow consumers to choose whether or not they wish to receive unsolicited commercial e-mail messages.

2) When consumers have indicated that they do not want to receive unsolicited commercial e-mail messages such choices should be respected.[44]

MEASURES TO REDUCE SPAM

A number of spam-reduction measures have been put in place by governments, ISPs and ESPs, e-mail marketers, businesses, anti-spam organisations, consumer protection associations, anti-spam solutions providers, etc. This section classifies these measures in terms of legal and regulatory approaches, self-regulatory approaches, education and awareness, and technical approaches.

Legal and regulatory approaches of member countries

There are basically two kinds of legal and regulatory approaches currently adopted to address spam. The first approach involves the application of existing laws and regulations which, though not specific to spam, may nevertheless be implicated by some aspect of spam. For example, laws to protect consumers from deceptive marketing or to prevent the distribution of pornographic images may be applied to spam messages. Likewise, data protection laws of general application could be implicated by spam practices. [45] The second approach involves the amendment of existing laws and regulations or the creation of new regulations to specifically address spam.[46]

Kinds of regulatory approaches

The summary below provides an overview of the main elements that can be found in OECD member countries that have taken the second approach and adopted specific regulations.

Opt-in

- The opt-in approach prohibits the sending of unsolicited electronic messages unless a prior relationship exists with the recipient or if the recipient has given his/her consent.

Opt-out

The opt-out approach may require any of the following:

- Explicit opt-out language be included in messages, or removal requests are in place (specific opt-out).
- The establishment of a “Do Not Spam List” (no-contact list, or universal exclusion list). Such a list allows senders of e-mail (particularly direct marketers) to remove from the list of their customers or prospects those consumers who have requested not to receive unsolicited e-mail (general opt-out).
- Clear and real identification of the sender, such as name, toll-free telephone number, valid sender-operated return e-mail address, postal address, or street address to allow for an easy way to opt-out.[47]

- Compliance with recipient requests to cease spamming them by immediately discontinuing spamming.

ISPs' right and responsibility

- ISPs can be given the right to deny services to spammers. Interactive computer service providers can be allowed to block commercial electronic mail in a specified manner.[48]

True identity and fairness; increased transparency

Regulation may include the prohibition of:

- False sender identities or addresses.
- False headers or misleading information in the subject line, or disregarding an opt-out request through technical manipulation.
- Unauthorised access or falsification of routing information or misrepresentation of information related to the identification of the point of origin or the transmission path.
- The use of a third party's Internet domain name without permission.

Labelling

- Labelling consists of displaying standard identifying labels in the subject line or header such as "ADV" (advertisement), "ADLT" (adult-only; if it concerns material intended for those 18 years of age and older).

Spamware

- Harvesting e-mail addresses from Web sites[49] can be prohibited and software products used for collecting e-mail addresses, transmitting bulk e-mail and falsifying return addresses (spamware) can be banned or controlled.

Scope of spam

- The coverage of spam laws and regulations may be restricted to e-mail, or expanded to include other electronic messages such as SMS and other forms of electronic messaging.

Disclosure or sale of personal data

- The sale, lease or exchange of certain personal identifying information obtained online without the knowledge or explicit consent of the consumer can be prohibited.

Summary of approaches adopted by OECD countries

Annex I provides details of OECD member countries' anti-spam legislation and Annex II shows these regulations in the form of a matrix. Eighteen member countries have specific laws or decrees on spam. Canada, Czech Republic, and Mexico, are applying existing laws and regulations to spam. Some countries such as New Zealand and Turkey have no specific regulations on spam yet. The following sections present an overview of the approaches adopted by OECD member countries.

Opt-in vs. opt-out

The paragraphs below introduce the EU member states' approach in a collective way first because they have similar legislative provisions with regard to privacy protection.

EU member states

The EU has adopted an "opt-in" approach for commercial communications by e-mail (including SMS), by way of Directive 2002/58/EC of 12 July 2002 *concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications), which is an integral part of the new, wider EC regulatory framework on electronic communications. Previously, the opt-in was applicable to faxes and automated calling machines.

The Directive contains three basic principles with regard to unsolicited commercial communications. Firstly, according to Article 13(1) of the Privacy and Electronic Communications Directive member states are required to prohibit the sending of unsolicited commercial communications by fax or e-mail or other electronic messaging systems such as SMS and Multi-media Messaging Service (MMS) unless the prior consent of the person has been obtained (opt-in system). This regime is applicable for marketing to individuals (natural persons) but member states can extend the scope to marketing communications to businesses. There is a limited exception from the opt-in system for existing customers [Art 13(2)], for the use of contact details obtained from customers in the context of a sale, but it may only be used by the same legal person for the marketing of 'similar' products or services and provide an explicit opt-out is offered at the time of collection and with each subsequent message. Secondly, the disguise of identity of the sender is prohibited. Thirdly, direct marketing messages must include a valid return address where persons may opt-out ('free of charge and in an easy manner').

"Electronic mail" is broad and technology neutral. It includes any form of electronic communication for which the simultaneous participation of the sender and the recipient is not required. Its definition covers not only traditional 'e-mail' but also SMS, MMS, etc.

The implementation of this Directive establishes a similar legislative model in all EU member states. Table 2 indicates the member states which have already adopted an opt-in approach.[50] Note that Finland, France and the United Kingdom do not require opt-in when the recipient is a registered legal person.

This Directive should be interpreted together with the 'general' Data Protection Directive 95/46/EC, where concepts like consent, etc. are defined. In addition to the above, other European Community law provisions may be applicable to unsolicited communications in relation to *e.g.* misleading advertising, harvesting, hacking.[51]

Table 2. **EU member states' opt-in/opt-out approaches to spam legislation**

Country	Unsolicited e-mails
Austria	Opt-in
Belgium	Opt-in
Denmark	Opt-in
Finland	Opt-in
France	Opt-in draft law
Germany	Opt-in
Greece	Opt-in
Ireland	Opt-in
Italy	Opt-in
Luxembourg	Opt-in draft law (document parlementaire 5181)
Netherlands	Opt-in draft law
Portugal	Opt-out
Spain	Opt-in
Sweden	Opt-in
United Kingdom	Opt-in

Source: OECD Secretariat and European Commission (2003), "Ninth Report on the Implementation of the Telecommunications Regulatory Package", 19 November, Annex 2, p. 29, http://europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/annualreports/9threport/annex2181103.pdf, accessed 9 December 2003.

Other OECD countries in Europe

Among the eight member countries which are in Europe but are currently not members of the EU, four are accession countries to the EU in 2004 and will have to transpose the EU directives: the Czech Republic, Hungary, Poland, and the Slovak Republic. The Czech Republic and Poland have already adopted opt-in and Hungary is currently in the process of adopting this approach. The Czech Republic has adopted the opt-in approach for commercial communications generally, but its legislation does not address spam explicitly. No information on the Slovak Republic is currently available.

As for the four other countries, Norway has adopted an opt-in approach. In Switzerland, following a public consultation in October 2002, the government is now amending regulation to apply opt-in to spam in all forms of messages (*e.g.* phone, e-mail, fax, SMS) and to oblige the telecommunication services providers to combat spam. There is no law on spam in Turkey, and information regarding the situation in Iceland is currently not available.

OECD countries in the Asia-Pacific region

Among the seven member countries in the Asia-Pacific region, Australia has been the first to introduce opt-in explicitly in their law. The April 2003 "Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered" recommending opt-in legislation was followed by the adoption of the Spam Bill 2003 by the Australian Parliament on 2 December 2003. Australia exempts government bodies, political parties, religious organisations, charities and educational institutions from respecting the opt-in requirement. There is no specific regulation on spam in Canada to date, though an opt-in approach has been adopted by applying existing law. In Canada, under the Personal Information Protection and Electronic Documents Act which came into force in January 2001, electronic mail addresses are considered personal information. Thus, the collection and use without consent of personal information, such as e-mail address, could run counter to the requirements of the Act.[52] Recent changes to the Federal Law of

Consumer Protection in Mexico reflect the adoption of an opt-out approach. Mexican consumers are entitled to prevent specific businesses from disturbing them at home or at the workplace, or via e-mail, and from unauthorised transmission of personal data to third parties.

To date, Korea and Japan have adopted an opt-out approach. However, on 19 October 2003, the Ministry of Information and Communication (MIC) in Korea announced the introduction of opt-in for mobile phone services. New Zealand has not legislated on spam yet.

The United States recently passed legislation on spam, which adopts an opt-out approach. It requires senders of unsolicited commercial e-mail to provide a mechanism to opt-out and requires senders to abide by recipients' requests to opt out. The legislation requires clear and conspicuous disclosure that the message is an advertisement. The senders must include a valid postal address in the e-mail and have a functioning e-mail address.

Other provisions related to spam

Not all of the OECD member countries have similar approaches to labelling and the use of spamware in their laws and regulations. With regard to labelling, Finland, Japan, Korea, Norway, Poland, United Kingdom, and the United States require senders to label certain kinds of messages, but others like Australia, Denmark, France, Germany, and Italy do not require it. Regarding the use of spamware, Australia, France, Italy, Japan, Korea, and Spain have a regulation which prohibits the use of spamware for the purpose of spamming, while others such as Denmark, Finland, Germany, and the United Kingdom do not. The United States prohibits the harvesting of e-mail addresses, dictionary attacks and spoofing.

However, concerning the real identity of senders, the provision of opt-out in messages, and false information in headers and messages, quite a few member countries have similar approaches. First of all, almost all responding countries which have spam regulations, including Australia, Belgium, Italy, Mexico, Netherlands, and Poland, indicated requiring the real identity and real address of a sender in their messages. One exception is Finland. The situation is similar regarding the opt-out requirement in messages. A few countries like Denmark, Finland, Germany, Italy, Korea, and the United Kingdom have a regulation in which opt-out is required in messages so that recipients are able to oppose receiving further messages from the sender. France, Mexico, Norway and Poland do not require this. A number of countries prohibit false information in headers and messages, including Australia, Denmark, France, Italy, Poland and the United States.

On the contrary, with regard to do-not-spam lists, most responding countries do not require the operation of do-not spam lists, with the exception of Austria and Korea. However, the United Kingdom, even though it is not a statutory requirement, opt-out registers have been operated under industry codes of practice. The US spam legislation requires the FTC to develop a plan and timetable for implementation of a do-not-e-mail registry and report any concerns about such a registry to Congress within six months of the enactment of the Act.

One more point worth mentioning is that sanctions for violation of spam laws and regulations are getting tougher. Some countries such as Korea have considerably increased existing fines imposed on spammers by amending existing regulations. Others like Italy impose not only fines on spammers but also prison terms.

Complaint mechanisms

To deal with complaints more effectively, some governments, such as Belgium, France and the United States[53] have set up dedicated e-mailboxes to which users can forward spam. By doing this, those governments are able to undertake legal action in targeted cases and also provide consumers with essential statistics about the size and nature of spam.

The limitations of regulation: the challenge of effective enforcement

There are a number of limitations to the effectiveness of law enforcement against spamming. These include low cost-effectiveness, difficulty in tracking spammers, difficulty in collecting evidence across borders, varying regulations between states and/or countries, etc. Some interpretations of existing privacy legislation can also raise obstacles to effective law enforcement, if they do not allow law enforcement to have access to information about alleged spammers.

The number of legislative initiatives in member countries suggests that legislation is a key tool for reducing spam. However, it is clear that legislation alone cannot address the problem. In addition, certain regulations, such as a labelling "ADV" in message headers (required by several state laws), has not proven effective as only 2% of spammers have complied.[54] Some organisations such as the Direct Marketing Association (DMA) argue that only legitimate law-abiding marketers would actually use ADV labelling, which voluntarily subjects them to mass filtering. Others also question the effectiveness of government-operated nationwide "do-not-e-mail registries", because such lists would only punish those reputable marketers who comply with them. On the other hand, according to a survey report of ePrivacy in July 2003, opt-out is not used by more than 37% of consumers. The primary reasons are: fear that opt-out will confirm their address to spammers; uncertainty as to whether opt-out will work; doubt that opt-out will be honoured.[55]

Spamming is a global problem, with e-mail being routed around the world. Because of practical problems in finding wrongdoers, establishing jurisdiction, and enforcing remedies, investigation and prosecution of cases involving spam are extremely difficult. Given the global nature of the Internet, the different approaches among countries may cause further difficulties to implement effective solutions worldwide. The spam outside their territories will be outside their reach.

There have been, however, a number of international initiatives to address the problem of cross-border scams. In particular, in June 2003, the OECD adopted new guidelines to foster international co-operation against cross-border fraud and deception *(OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders)*. Spam messages that contain deceptive or fraudulent representations may fall within the scope of the guidelines, offering the prospect of putting into play the framework for enforcement co-operation outlined by the guidelines.

Self-regulatory approaches

There are a variety of ongoing self-regulatory efforts in place to reduce spam. Some of the current private sector initiatives are provided below; including those by anti-spam organisations, ISPs, ESPs, the Internet industry, e-mail marketing companies, consumer protection organisations and end-users.

The self regulatory activities of major participants

Initiatives of anti-spam or Internet user organisations

Many anti-spam organisations provide a list of, or link to, other anti-spam organisations on their Web sites. Annex IV sets out a list, as provided by SpamCon Foundation. These organisations try to raise awareness by providing users with information or resources on spam, statistics and legislation regarding spam, and suggestions for how to identify and reduce spam. One such organisation, Spamhaus,[56] provides technical tools for blocking spam or tracing spammers, as well as a blacklist of well-known spammers. Other organisations, such as the Coalition Against Unsolicited Commercial E-mail (CAUSE), are active participants in the legislative debates.[57] Still other organisations, like the SpamCon Foundation Law Center and SpamLaws.com, provide information on existing spam-related laws and/or how to take legal action against spammers. Others operate reporting centres that receive complaints on spam, and analyse or forward the spam to the appropriate authorities for further investigation. Other organisations provide best practices or encourage ISPs or online marketers to enforce strong terms and conditions which prohibit spam.

Internet user organisations are also working to fight spam. The Spanish Internet Users Association has been operating an anti-spam Web site (http://aui.es/contraelspam). This site complements other initiatives it has taken to fight spam, that include tracking the evolution of spam, awareness campaigns, developing a co-ordination centre for ISPs, and developing tools to help users analyse and filter spam.

Consumer organisations have also taken initiatives. For instance, the Trans Atlantic Consumer Dialogue (TACD), a coalition of more than 60 consumer organisations from the United States and EU member states, has adopted a resolution[58] that calls for common approaches to the international problem of spam. The resolution strongly supports an opt-in approach, recommending that commercial electronic communications only be sent with prior affirmative consent of the recipients.

ISP, ESP and Internet-industry initiatives

As major victims of spamming, ISPs and ESPs have taken some preventative and punitive actions against spamming. The vast majority of ISPs and ESPs have implemented technical measures like filters to detect incoming spam and launched user-generated blacklists to staunch the flow of spam.[59] By doing so, they try to prevent bandwidth and system-resource drain, and to assist consumer efforts to reduce spam. However, the use of filtering devices raises the issue of the legitimacy of a private ISP's decision to block messages from a particular sender. In addition, filters do not work when the sender's e-mail address has been masked or falsified. On the other hand, ISPs maintain the right to terminate the account of any subscriber who engages in abusive e-mail practices in their terms of agreement.[60] A US ISP has included in its user contracts a provision stating that a subscriber could be charged up to USD 50 for each delivered spam mail message.[61]

The Canadian Association of Internet Providers (CAIP) has developed a voluntary code based on its membership's best practices. Competing for subscribers, ISPs are free to establish their own acceptable use policies and to enforce them under their terms of service agreements. According to the CAIP, the vast majority of its member ISPs already prohibit the use of their networks for bulk electronic mailing and reserve the right to terminate the account of any subscriber who indulges in this activity.[62] Some ISPs try to reduce the capacity for spammers to utilise anonymous accounts through the appropriate implementation of technologies such as Caller Line Identification (CLI), and encourage identification requirements for prepaid accounts. Other Internet industry associations like the Advertising and Commercial Internet

Industry Mexican Association have developed codes of practice that cover the use of personal data for marketing purposes.

A major incentive for spamming is its low cost for the sender. Some ESPs have attempted to address this on a commercial basis, *e.g.* attempted to reduce spam and obtain financial compensation from spam. For example, Daum, a Korean ESP, has established the "online stamp system" since April 2002 to reduce spam sent to their users.[63] It arose from the theory that spam would be dramatically reduced if commercial bulk e-mail senders were obliged to pay for sending spam. It has been suggested that as a beneficiary of bulk commercial e-mail, the sender should share the cost of network infrastructure.

The Internet industry has also launched educational awareness campaigns to help users understand spam and how to reduce it. For example, the Internet Industry Association in Australia launched a programme involving 11 anti-spam software vendors, who agreed to provide free month-long trials of their products to all Australian Internet users on 16 April 2000.[64] The Australian telecommunications industry also developed a code of practice regarding SMS spam in 2002. Finally, public services such as GetNetWise (http://spam.getnetwise.org) operated by Internet industry corporations and public interest organisations help people counter spam by providing useful tips and solutions.

Also, lawsuits against spamming are increasing. Recently more companies have tried to sue spammers in civil court for losses due to the spamming. For instance, in 2003, Microsoft Corp. moved to curtail unsolicited e-mail by launching dozens of lawsuits in the United States and the United Kingdom against companies that sent more than two billion spam messages to the software giant's customers, many of whom use its free Hotmail service. EarthLink recently filed a $5 million lawsuit against 100 alleged spammers. These kinds of legal initiatives by ISPs may deter spammers.

E-mail (or online, direct) marketing company initiatives

Proliferation of opt-out lists. An individual's express wish not to receive spam in itself constitutes valuable information which when shared among retailers enables them to reduce unproductive marketing expenditures and avoid negative responses and complaints. In some European countries, opt-out lists are being put in place either by national direct marketing industry federations, the Federation of European Direct Marketing (FEDMA), or by newer organisations representing the online industry. Created in France in 1998, opt-out lists have been actively promoted by the *Fédération des Entreprises de Vente à Distance* (Direct Marketing Federation - FEVAD) since the summer of 1999. It is a potential model for other national opt-out lists, and an agreement has been signed with the German Direct Marketing Federation to this effect. The *Association Belge du Marketing Direct* (ABMD) has also set up a nationally-based general opt-out list.

Almost all these initiatives were taken in response to the adoption of Directive 2000/31/EC on e-commerce, Article 7(2).[65] According to a comprehensive survey of European industry federations conducted by the European Commission from May to October 2000, opt-out lists had been set up in Finland, Germany, Italy, the Netherlands, Norway, Spain, Sweden, and the United Kingdom. They were initially designed to cover only the particular member state concerned, but most of the federations behind the initiatives plan to extend these national opt-out lists in the near future to the EU as a whole and possibly to countries outside the EU.[66] However, as the EU member countries have adopted opt-in in their law according to the Directive 2002/58/EC, it is not clear whether opt-out list operations will nevertheless continue to extend in those countries.

The Direct Marketing Association (DMA) in the United States has also introduced a self-regulatory preference scheme for consumers (an opt-out scheme) operated by the association itself. Consumers can

register their wish not to receive spam in the e-Mail Preference Service (e-MPS), operated by DMA, then all DMA members who wish to send unsolicited commercial e-mail must remove the individuals who have registered from their prospect e-mail lists.[67] Mobile phone numbers may also be registered free of charge with the UK Telephone Preference Service (though this is now partially overtaken by new opt-in rights for SMS).[68]

Opt-in (prior permission or consent-based) direct marketing. More and more e-mail and directing marketing companies have adopted the principles of permission-based marketing and opt-in e-mail. For instance, in October 2000, the Finnish Direct Marketing Federation adopted a code of conduct requiring an opt-in approach. The e-mail address collection model is to post opt-in forms on Web sites. Visitors complete the online forms in order to subscribe to a newsletter, take part in a competition or promotion, or receive special offers in line with the interests they register. Quite a few Web sites now provide their visitors with two choices: *i)* to indicate whether or not they wish to receive commercial messages; *ii)* to indicate if their data can or cannot be disclosed to third parties. Opt-in direct marketing practices, especially by legitimate marketers, seem to be growing dramatically in the member countries that have adopted, or are in the process of adopting, an opt-in approach, *e.g.* in Australia and EU member countries.

Codes, guidelines and/or other policy commitments. The direct marketing associations have also drafted guidelines, such as DMA's Commercial Solicitations Online Guidelines which cover sending commercial e-mail, including under what circumstances e-mail can be sent, the use of e-Mail Preference Service, and establishing the clear identity of the sender.[69] Associations such as the Canadian Marketing Association (CMA) have established codes and sets of guidelines for their members which deal with the use of Internet for the distribution of promotional materials.[70] Some associations, such as the Network Advertising Initiative (NAI), a co-operative group of network advertisers, and the Association for Interactive Marketing (AIM), a non-profit trade organisation have developed a set of privacy principles.[71] They also provide advice on how to reduce the amount of spam to consumers and companies. Some companies have adopted policy measures which enable the recipient of an e-mail identified as commercial to be listed in an opt-out register by simply clicking on a link placed at the end of the message.

Limitations of self-regulatory approaches

Although self-regulatory approaches may be a critical step in spam prevention, there are a number of limitations. Few spammers are members of the Internet Industry Association or are likely to adhere to its code voluntarily. Unfortunately, a code of conduct provides only limited protection against "bad" spammers. Spammers easily find methods to avert systems and/or punitive self-regulatory action, *e.g.* creative use of programming, switching ISPs, falsifying their identities, etc.

Education and awareness

Consumer education and awareness, accompanied by other solutions, may have an important impact on alleviating spam. Not only could awareness turn numerous spam victims (who unknowingly disseminate their addresses on public spaces to spammers) into spam-free users, but it may also increase e-mail address collection costs for spammers, making spam less profitable. Education is also a solution that spans geographical borders. Legislation is limited in its ability to protect a user from a foreign spammer, but steps taken by an informed user will help regardless of where the spammer is located.

In this regard, many consumer protection organisations have provided educational and awareness-raising programmes to empower consumers to make informed choices in relation to spam reduction strategies and technologies. These activities and programmes, in most cases, have been carried

out in conjunction with other e-security initiatives such as anti-virus, e-privacy or consumer protection initiatives.

Many consumer protection organisations have raised public awareness by informing consumers about spamming tactics and providing them with suggestions on how to prevent spam. For example, the Center for Democracy and Technology (CDT) recently released a report on the most successful methods for preventing the reception of unsolicited messages, *e.g.* through obscuring e-mail addresses or hiding them altogether.[72] The report emphasised that consumers should be aware that certain areas of the Internet, like newsgroups, have little or no security. Other organisations have taken initiatives to help people technically online or on site to prevent spam. For instance, the Korea Information Security Agency has developed strategies to check weak points in the private sector and aided users in performing self-checking activities so as to shut down open relay mail servers, as early as 2002. Another interesting initiative is the development of a tool called a "verified sign", *e.g.* Trusted Sender message, which aims to authenticate the sender, the integrity of the message, etc.[73] Some consumer associations provide a black list of spammers. One example is a black list published by *L'Union Fédérale des Consommateurs de Quimper*, a French Consumers Association, in its *Arnaques-infos*.

As one of the main players in the development of public awareness and education on spam, regulatory agencies and governments have also developed comprehensive guides for business and individuals on how to prevent spam, and how existing legislation can be applied to counter spam. Many governments have been encouraging industry stakeholders to deal with spam through voluntary industry-wide codes and practices. For example, the Australian Department of the Treasury has developed an "Australian E-commerce Best Practice Model" for all online businesses, which contains provisions specific to direct marketing over the Internet.[74]

The US FTC operates a Web site dedicated to spam awareness, which provides information to users on how to respond to spam. The French Data Protection Authority has posted on its Web site substantial information on a variety of aspects of spam. The European Commission also has a plan to provide information on its EUROPA Web site including its member states' regulation, hyperlinks to national sites, and figures and trends on spam in the EU in the near future. In addition, the European Commission has developed a Safer Internet Action Plan to foster co-ordination of awareness-raising activities and programmes in member states for the safe use of the Internet.

ISPs and Internet industries have also promoted user awareness and education. For example, Microsoft has launched MSN Spam Buster,[75] a spam education Web site that advises Internet users how to protect themselves against spam, including the use of e-mail filters.

Technical solutions

As the volume of spam has increased rapidly and entry costs for vendors have been low, anti-spam products have increased. Many new products and services have recently come on the market, aimed at providing technical solutions to individual users, service providers and organisations. Some of the technical tools that may help filter or block unwanted e-mail messages are noted below.

Current e-mail structure

One of the major technical reasons why spam is so prevalent is that SMTP (Simple Mail Transfer Protocol), which is the protocol used for transmitting messages between servers (or from a mail client to a mail server), does not verify the validity of the sender identifier, such as the "sending server" and the "from" address. These two identifiers are the only identity information received before the mail is

delivered under SMTP, and both of those identifiers can be falsified. In addition, no mechanism exists to verify the integrity of the body of an e-mail. The contents of an e-mail including the subject and other information are transmitted in a data block and are not considered a meaningful part of the SMTP conversation.[76] Ignoring content leads to high efficiency (read high volumes of global e-mail traffic) in this case, but with no checks and balances in place, it also raises questions concerning trust and accountability. With no accountability, spam flourishes.

Deployment of anti-spam services and technology

Anti-spam solutions protect and help business, ISPs and individual users to reduce the amount of time spent reading and managing unwanted e-mail by filtering out inappropriate and offensive content. One of the solutions is through filters using "blacklists", which consist of domain names or Internet protocol (IP) addresses of known spammers. Blacklists can be established in a collective way. Once enough recipients in a certain user community object to a particular message, the message is automatically transferred to future users' spam folders. Another technical option, "white list", or "approved sender lists", allows users to identify e-mail from approved and legitimate senders. While white lists can help refine spam filtering, they are currently prone to spoofing, or falsification of e-mail source data. Another technical tool suggested as having good anti-spam potential is to set one's e-mail client to accept only messages signed with trusted digital certificates issued by a trusted certificate authority. Digital signature schemes such as public key infrastructure solutions can be used for this purpose.

In addition, there are other anti-spam tools, one of which is behavioural analysis tools that look for patterns such as large numbers of recipients. Address-validation tools reverse domain name system lookups to ensure the sender is not trying to cloak his identity. Digital fingerprints developed with algorithms and heuristics are also used to identify and block or filter common spam patterns.

New products are emerging on the market that can scan for graphics such as skin tones to combat pornography, but these tools are still in their infancy.[77] Another new technique, called Bayesian filtering, learns and relearns how to spot spam by scanning the mail users have read and the mail users have rejected without adhering to any particular set of rules. Then it calculates probabilities based on each e-mail's unusual characteristics and decides what kind of e-mail to deliver and reject. This can be a viable solution because only recipients know what they are interested in. It is expected to be 99% accurate and released commercially in 2004. Another new technology recently introduced is a challenge-response technology, which uses a tactic that requires a sender to verify his or her identity before being added to a "white list" that enables him or her to send e-mail unrestricted in the future.

Most anti-spam solutions usually include a combination of several technical components, such as heuristic rules-based scanning, white and black lists, content-analysis tools, other key security features like SMTP-based authentication,[78] and configurable network-based updates to heuristic rules engines[79] as new filters allow devices to keep up with spammers. Generally speaking, to identify spam, anti-spam solutions not only compare e-mail addresses to a list of known spammers but also perform full content analysis of the entire e-mail message by looking for common commercials and pornographic text patterns. Anti-spam solutions also apply "fuzzy-logic" filters to each e-mail message examined under the control of the user. In addition, anti-spam solutions are automatically updated, as spam techniques evolve quickly.

Efforts by technical expert groups

Efforts to find technical solutions to spam prevention/reduction have been made at the individual company level and by many companies in a collective and co-operative way. As spam becomes a major issue, more and more technology companies have discussed solutions to counter spam. An industry

anti-spam conference was held on 27 February 2003 to co-ordinate an industry-wide approach to the problem. At the conference, attendees from every technology and business sector with an interest in spam began to contemplate a more holistic approach to the problem. The idea for the project was for the technology industry to work together to produce an open, interoperable anti-spam protocol that would work between all e-mail systems of a dissimilar origin and would stop spam while guaranteeing safe passage for legitimate mail.[80]

Equally, several major technology companies including Yahoo, Dell Computer, Oracle, Microsoft and Sun Microsystems met on 14 March 2003 in San Francisco to discuss solutions to spam. The goal of the forum, called JamSpam, was to create an open, interoperable anti-spam specification that would serve as a universal solution to spam. The discussions at the meeting included developing e-mail authentication standards to ensure that legitimate messages are recognised and delivered securely. In a special meeting of ISPs and ESPs, the various companies discussed technological solutions to closing open relays. Companies were also interested in building a system where there would be more transparency for legitimate messages sent, *i.e.* discernment of the nature of a message - whether the e-mail is a newsletter, a bill from an e-commerce site or a message from a friend.

In April 2003, Microsoft, AOL and Yahoo announced that they were working together to block unidentified messages and to stop spammers from creating fraudulent e-mail accounts. In addition, some ISPs also gathered together to find technical solutions for spam. For example, Poland's biggest Internet portals and e-mail service providers – Onet, Wirtualna Polska and Interia formed a coalition to try to stop spam sent through their systems in May 2003. The three companies drafted a common plan of action to develop new technology that would restrict individuals and companies from sending spam.

The discussions on anti-spam technology continue. An influential Internet standards-setting body began a close scrutiny of the mounting problem of e-mail spam, in an effort that could have broad-ranging implications for future e-mail use and security. An official Anti-Spam Research Group[81] was convened under the auspices of the Internet Research Task Force, an informal organisation affiliated with the Internet Engineering Task Force (IETF). The new group is an open research body without policy-setting power, but its findings could ultimately change the way e-mail is handled by ISPs and networks. On the other hand, on 16 September 2003, chief executive offices and executive decision makers from 40 companies such as ISPs, spam filtering companies, and e-mail senders gathered together in the E-mail Deliverability Summit in San Francisco to address the issues of false positives and improve deliverability rates for legitimate e-mail, while enabling receiving systems to identify spam. Some standards related to bounce handling, unsubscribe requests, publication of e-mail permissions requirements, and communication between the sending and receiving industries were presented. [82]

Limitations of technical solutions

The majority of spam-blocking technologies currently use keyword or blacklist blocking, which results in a large number of false positives. False positives occur when a legitimate e-mail is mislabelled as spam and filtered. The possibility always remains that all messages originating from a blacklisted site are systematically deleted without being delivered.[83] In addition, anti-spam blacklists often block innocent Internet users connected through blocked ISPs. There have even been cases of entire country domains being blocked. While some users have felt empowered by these filters, many ISPs argue that they have had the effect of victimising the wrong people, including ISPs that host spammers unknowingly, Internet users who may have been spoofed by a spammer, and addresses adjacent to the alleged spammer.

To counter this problem, anti-spam solution companies provide various methods such as heuristic rules-based scanning and fuzzy-logic filters. However, whether or not a particular message is spam is very

hard to determine through purely automated processes. Computer algorithms to identify spam are far from perfect. Moreover, the problem with relatively newly introduced technologies such as challenge-response technology is the extra burden they place on legitimate senders. In addition, the list owners of many subscribers such as newsletter mailers (automated response systems) have difficulty answering challenge-response e-mails personally, so subscribers may find their newsletters getting stopped. This makes for a kind of false positive.

Another approach to spam filtering is the consensus model, whereby people who receive messages that they consider to be spam report them as spam to a co-ordinating entity. A computer program is then used to co-ordinate all of the input. A properly compiled list of known spammers would also be a significant improvement on unregulated blacklists that currently operate. Nevertheless, perfect filter systems are nearly impossible to deliver.

Many spammers are technologically sophisticated enough to cover their tracks, adjust their systems to slip through filters and scale other technological barriers. They can electronically commandeer unprotected computers, turning them into a tool for their own spamming. As long as spam costs are so low, spammers have a vested interest in finding ways to defy technological limits.

Anti-spam solutions do inevitably add additional cost and latency to ISPs, ESPs and consumers. An effective e-mail filtering service can entail considerable added costs for service providers and they often have some side effects on the efficiency of communications. Filtering messages costs ISPs time and money and slows network performance. Some ISPs consider that filter products are worthwhile, at least at the consumer level, but are not always easy or desirable to design, configure or install at the ISPs level.[84]

CONCLUSION

The low cost and global reach of e-mail and other electronic messages have made them an extremely important and popular means of communication. However, the rapid growth in spam threatens the convenience and efficiency of electronic messages and undermines user confidence online more generally. A variety of measures and initiatives have been undertaken in OECD countries to address the recent surges in spam volumes and reinforce consumer confidence online. It does not appear, however, that these regulatory, self-regulatory and technical measures have yet been successful in slowing the growth of spam. Renewed efforts to tackle this problem will need to recognise that no single approach will likely succeed in stopping spam, and that international co-ordination will be needed to address a problem that does not recognise national boundaries.

A multi-dimensional approach needed

No current approach to addressing spam is without its own limitations. Legal approaches confront the difficulty that senders of spam are often effective in hiding their identities and operating across borders. Self-regulatory approaches are challenged to ensure that spammers voluntarily participate and abide by industry codes of practice. Greater public awareness and education are needed to foster safer computing practices. In this respect, anti-spam strategies might be linked to general e-security campaigns. On the technical side, continued support for the development and deployment of technical tools to fight spam is needed to help ensure that spam does not elude the filters of ISPs and others. On the whole, a blended approach combining regulatory, self-regulatory, technical solutions and user awareness offers the best prospects for reducing spam.

International co-operation is also a critical factor

Spam is not the problem of any single country, or even limited to OECD member countries. It is a worldwide problem. With Internet access and use continuing to grow in developing countries, the global character of spam may yet expand further. It is increasingly clear that domestic efforts must be supplemented by internationally co-ordinated strategies to address the cross-border challenges posed by spam.

ANNEX I. NATIONAL LEGISLATION

Australia - Opt-in

The SPAM Bill 2003 was passed by the Australian Parliament on 2 December 2003. The bill adopted an opt-in regime for commercial electronic messaging. Electronic messages include e-mails, instant messaging, text or video messaging to mobile phones and messages defined in the regulation. It also requires accuracy with regard to address of sender and a functioning unsubscribe facility; it prohibits the distribution and use of electronic address harvesting tools and harvested address lists; and encourages the development of appropriate industry codes. A flexible and dynamic civil sanctions regime such as warnings, infringement notices and court-awarded penalties is addressed in the bill as well. The spammers who contravene the legislation will be liable for up to a total of AUD 44 000 for contraventions on a single day, while an organisation could be fined up to AUD 220 000 a day. Directory harvesting and dictionary attacks, when conducted for the purposes of engaging in spam or associated activities, are also banned under this legislation. The Australian Communications Authority (ACA) will have the power to investigate, issue infringement notices and institute proceedings. Where a person or company has suffered loss or damages due to a spammer's activity, the ACA may apply to the court on their behalf for compensation.

Austria - Opt-in

Section 101 of the Telecommunications Regulation Act (Austrian Official Gazette n° 100/1997) requires prior consent for bulk e-mail for commercial purposes.[1] Under Article 7(2) of the e-commerce Act ("*Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts-und Rechtsverkehr geregelt werden")*, the *Rundfunk und Telekom Regulierungs* has compiled an opt-out list which lists those who are not willing to receive commercial e-mail correspondence, open to all users.[2]

Belgium - Opt-in

Belgium adopted an opt-in approach for "commercial electronic mail" in the Law on Electronic Commerce of 11 March 2003. The act requires information about the option to object to further advertisements via electronic messaging. It also prohibits the sender from using e-mail addresses from third parties without the consent of the data subject, and from falsifying or concealing the sender identity. The sender has to prove that there was a request for advertisement e-mail.

Canada - Opt-in approach, applying existing Act

Before the Personal Information Protection and Electronic Documents Act was legislated, the Canadian government took the position that the distribution of unsolicited promotional and product information, in print form or electronically, was not illegal, nor was it regulated in Canada.[3] However, under the Act which came into force in January 2001, electronic mail addresses are considered personal information and thus subject to the provisions of the Act. The collection and use of personal information (such as e-mail addresses) without the consent of the data subject could run counter to the requirements of the Act. The Privacy Commissioner of Canada is entrusted with enforcing the Act.

The law also creates an obligation for firms and others who store electronic mail addresses to provide appropriate security for this personal information. In the first three years following the Act's adoption, the legislation applies to federally-regulated undertakings and to private sector firms who engage in inter-provincial and international trade in personal information. After this time, all organisations using personal information for the conduct of commercial activity will be covered. Thus, firms buying, selling, leasing or bartering electronic mailing lists, which are the basis for bulk unsolicited electronic mail, will be subject to the provisions of the legislation, if these transactions take place over provincial and national borders.[4] However, there is no specific regulation on spam to date.

Also, although there is no specific legislation dealing with spam in Canada, spam which conveys misleading representations or deceptive marketing practices could breach sections of the Competition Act and other statutes enforced by the Competition Bureau in Canada.

Czech Republic - Opt-in approach, applying existing Act

The problem of spamming is generally described in Article 2 of the Act No. 40/1995 Coll. on the regulation of advertising. It is forbidden to send unsolicited commercial communication if it represents any expenditure on the part of the recipient or if it disturbs the recipient. The recommendation on spamming in the draft version of the White Paper on e-Commerce was to be submitted to the government for approval in the second quarter of 2003. Most targets defined by the Directive 2000/31/EC have been transposed into the Czech legal framework. The government is now focusing on those requirements that have not yet been met.[5]

Denmark - Opt-in

Denmark has adopted an opt-in model with modifications. The Danish Marketing Practices Act requires that the customer, prior to receiving the "call using mail", has *requested* the call. A new section effective from 25 July 2003, modifies the rule, allowing a supplier having received a customer's electronic address in connection with the sale of a good or a service to send unsolicited e-mail without the customer actively requesting it, when a number of clearly defined conditions are met. The customer must be able to opt-out easily and free of charge at any time. The new paragraph applies only to electronic messages. Danish legislation also requires a real identity and address as well as an opt-out option in messages, and prohibits the falsification of information in headers and messages.

Finland - Opt-in

The new Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector was issued on 12 July 2002. The national implementation of the law in Finland is in its final stages. The Directive will be brought into force with the new Finnish Act on privacy in electronic communications. The government reached its decision on the content of the law on the protection of privacy and data security in electronic communication on 15 October 2003. The bill was put before Parliament on 24 October. The bill is currently being discussed by the various parliamentary committees. The parliamentary committee on transport and communications will present its statement on the government proposal probably in March 2004. The bill may become law in spring/early summer 2004.

According to the new law proposal, direct marketing by means of automated calling systems; facsimile machines; e-mail, SMS, voice, sound or image messages is only allowed in respect of natural persons who have given their prior consent. (However, where a service provider or a seller of a product

obtains from its customer, who is a natural person, their contact details for e-mail, text, voice, sound or image message in the context of the sale of a product or a service, the same service provider or a seller of product may use these contact details for direct marketing of its own products of the same product group and other similar products or services. The service provider or a seller of the product shall give its customer, who is a natural person, the opportunity to refuse, free of charge and in an easy manner, the use of contact details when they are collected and the occasion of each e-mail, text, voice, sound or image message.)

The new law doesn't require opt-in for legal persons, but it requires labelling and an opt-out facility in messages. It prohibits false information in headers and messages. It prohibits sending direct marketing messages that disguise or conceal the identity of the sender or have invalid addresses. Telecommunication operators and corporate and association subscribers would have the right to filter out illegal marketing e-mail and malicious programs in order to ensure communication services. With the user's consent, disruptive e-mail could be filtered out to a larger extent.

The opt-in approach in respect of natural persons has been required since 1999 based on the act 1999/565 on the Protection of Privacy and Data Security in Telecommunications. This act does not require opt-in for legal persons. A subscriber who is not a natural person can forbid it. The act also provided that direct marketing directed at a consumer shall further be governed by the provisions of the Consumer Protection Act (1978/38). On the basis of the Consumer Protection Act, the sending of electronic direct marketing without the prior consent of the consumer is also regarded as unfair marketing.

The above mentioned new Finnish Act on privacy in electronic communications will replace this act 1999/565 on the Protection of Privacy and Data Security in Telecommunications.

France - Opt-in bill in progress

A new bill, *Pour la confiance dans l'économie numérique*, was introduced by the French government in January 2003, adopted by the National Assembly on 26 February 2003 and by the Senate on 25 June 2003 and is still in the legislative process. Article 12 in the bill adopts the opt-in approach for e-mail targeting individuals. However, there is still debate between opt-in and opt-out in respect of registered legal persons. Nevertheless, e-mailing for commercial purposes without the recipient's prior consent is authorised if data concerning the recipient have been gathered from the recipient directly in the context of an existing commercial relationship. In all cases, full compliance with French data protection law is mandatory, and the sender of commercial e-mails must include a clear and easy way for the data subject to oppose the use of his/her e-mail address.

It also requires a real identity and address for senders, and prohibits false information in headers and messages. The bill designates the National Commission of Information and Liberties (CNIL) to handle complaints about spam from individuals.[6]

Germany - Opt-in bill in progress

Germany is in the process of legislating an opt-in bill, an amendment to the Law on Unlawful Competition *(Gesetz gegen unlauteren Wettbewerb §7 UWG)*. Its purpose is to implement Article 13 of the EU Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002/58/EC of 12 July 2002). The bill provides - in particular a new Section 7 of the Law on Unlawful Competition – that sending unwanted advertisements by e-mail, fax or automatic calling machines without prior consent of the addressee constitutes unfair competition. The provision will

be applicable irrespective of whether the addressee is a natural or a legal person, thus protecting companies and consumers alike. A claim against the unlawful competitor can be asserted by any of his competitors, by associations representing the interests of companies offering comparable products or services, by the chambers of commerce as well as consumer organisations. They can request the unlawful competitor to stop the unfair behaviour and to refrain from it in the future. If any profit was made, the organisations named above can also ask for this profit to be paid to them. Competitors affected by unfair competition can claim compensation.

If a company has acquired an electronic address due to a prior commercial relationship, the company is entitled to use the address for the purpose of sending advertisements for comparable goods or services unless the customer disallows him to use his address (opt-out). At the time when the address is acquired and every time the address is used, the consumer must be informed that he can disallow the use of his address at any time. A violation of this rule also constitutes unlawful competition.

Even prior to the introduction of the proposed bill, Germany had an opt-in requirement. Unsolicited calls for commercial purposes are prohibited under the Law on Unlawful Competition. According to a number of court rulings, this also applies to unsolicited e-mails, but there has not yet been a ruling from the highest court on this matter.

Greece - Opt-in

Opt-in is required for unsolicited e-mails, calls and faxes for advertising purposes.

Hungary - Opt-out

Although not specifically related to the Internet, Hungarian law provides for some restrictions regarding unsolicited commercial communication. The Government Decree Nr. 17/1999 (II. 5.) on distance selling prescribes that unless the consumer explicitly objects, a business may use a means of telecommunication that enables direct contact between parties, but does not fall within an offer made by telephone or fax. As a consequence, the use of spam is not admissible if the consumer explicitly objects to it.

According to the Act on Advertising, the advertisement may only be published if its advertising nature is clearly indicated and separable from the rest of the communication.[7]

Ireland - Opt-in

The SI No. 535 of 2003 European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations came into force on 6 November 2003. The main features of the regulations are:

Right of subscribers to determine which of their personal data are included in publicly available directories of subscribers.

Requirement that subscribers are informed of the purposes of public directories before they are included in them and given complete information about the ways in which their personal data can subsequently be used or accessed.

Provision for the processing of mobile location data, with subscribers consent, for providing new value added services.

Confidentiality provisions extended to the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber. The use of cookies and other devices such as spyware are regulated and require the consent of users.

Restrictions on unsolicited direct marketing by telephone, fax, automated calling systems, e-mail, SMS and MMS. Spam (originating in the EU) sent to natural subscribers will be illegal. Business subscribers and other entities will also have enhanced rights regarding the prevention of spam.

Provisions for enforcement of regulatory decisions by Comreg and the Data Protection Commissioner, including powers for investigations of suspected breaches of the regulations.

Spam sent to individuals, with a limited exception (covering existing customer relationships) is only allowed with prior consent. This "opt-in" approach equally covers SMS messages and other electronic messages sent to any mobile and fixed terminal. Under the regulations, individuals found responsible for creating spam or unsolicited e-mails and text messages could face up to EUR 3 000 per message, and possibly a prison term in the future.

Italy - Opt-in

In Italy, prior consent for sending unsolicited communications, including via e-mail, has been mandatory since 1998 – under Section 10 of Decree no.171/1998, implementing the EC Directive 97/66, as well as under Section 10 of Decree no. 185/1999, implementing the EC Directive 97/7 on Protection of consumers with regard to distance selling.

The new Data Protection Code, in transposing Directive 2002/58/EC into Italian legislation, confirms the opt-in approach already laid down in the aforementioned decrees. Furthermore, the new code (in particular, Section 130) regulates unsolicited communications in a much more detailed way, explicitly embracing all kinds of unsolicited communication (e-mail, faxes, MMS, SMS, etc.) and setting sanctions that may even be criminal in nature.

The new code prohibits the practice of sending communications for commercial or promotional purposes by disguising or concealing the identity of the sender, or without a valid address to which the data subject may send a request to exercise his rights. Section 130 also allows the *Garante per la protezione dei dati personali* (the Italian Data Protection Authority), in cases of persistent breach of the provision, to order the provider to implement filtering procedures or other practicable measures with regard to the electronic contact details for electronic mail used for sending the communications. As far as self-regulation is concerned, Section 133 allows the *Garante* to encourage the adoption of a code of conduct and professional practice applying to the processing of personal data by providers of communication and information services supplied by means of electronic communications networks.

The *Garante* has adopted numerous decisions on spamming, often blocking the processing of personal data stored in the databases of the companies using e-mail addresses unlawfully. Furthermore, on 29 May 2003 the *Garante* adopted a general measure concerning unsolicited messages sent for direct marketing, advertising and promotional purposes. The opt-in principle was reaffirmed, by stating that e-mail addresses which are publicly available on the Web, on discussion groups or on registrars' directories are not to be used to send unsolicited messages, unless the addressee has given his prior consent and has been informed of the rights arising from the data protection law. Therefore, the *Garante* prohibited further unlawful data

processing aimed either at sending advertisements or carrying out direct marketing activities, or performing market polls or interactive commercial communication.

Japan - Opt-out

In July 2002, two laws regulating spam came into effect. One is the Law on Regulation of Transmission of Specified Electronic Mail (Law No. 26 of 2002), which aims to regulate the transmission of unsolicited commercial e-mail. The law obligates senders of unsolicited e-mail to display the sender's name, contact information, and state at the beginning of the subject line if the e-mail is an advertisement that was neither consented to nor requested so that users have the option to automatically block all mail that contains unsolicited advertising. The law also prohibits the transmission of e-mails to randomly generated e-mail addresses. In addition, the law prevents senders from e-mailing recipients who have informed senders by phone or e-mail that they do not wish to receive e-mail from them. The Minister of Public Management, Home Affairs, Posts and Telecommunications issues administrative orders to compel illegal senders to comply with the law. If a sender violates the law after receiving the order, a JPN 500 000 (USD 4 180) fine for non-compliance may be imposed. The law allows telecommunication carriers to refuse e-mail from spammers if it creates system problems. The Minister has issued several administrative orders since the law came into force in July 2002.

The other is an amendment to update the 1976 Specified Commercial Transactions Law (Law No. 28 of 2002), which governs mail-order sales and was instituted in order to protect consumers from exploitive marketing techniques, such as direct marketing. It provides users with an opt-out option, requiring sellers of products or services provider which advertise through e-mail to display their name, contact information, and state at the beginning of the subject line if the e-mail is an advertisement that was neither consented to nor requested so that users have the option to automatically block all mail that contains unsolicited advertising. It also requires them to attach messages informing recipients how to reject future ads. Once the ads have been rejected by recipients, sellers of products or service providers are prohibited from sending the ads again. The Ministry of Economy ,Trade and Industry sends warning messages to sellers of products or services providers who are likely to violate the law (3 700 messages were sent in 2002), and imposes governmental orders on them if they don't obey warning messages (two companies received such orders in October 2003). Violations of this new law will result in maximum prison terms of two years or fines up to JPN 3 million (USD 24 000).[8]

Korea - Opt-out

The Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection prohibits transmitting spam against the addressee's express wishes. It also prohibits disregarding an opt-out request through technical manipulation. The Act prohibits transmitting spam such as adult advertisement via e-mail, telephone, facsimile, or others to juveniles. The act of spam is sending any commercial advertisement via e-mail, telephone, facsimile and so on to a user against the user's express rejection in violation of the law. The Act also requires the sender to expressly indicate the objective of transmission and major contents thereof, the name and contact means of the sender, and an opt-out option. The Act requires labelling "ADV" or "ADLT" in headers and clear expression about a method for refusal of future messaging, name, telephone number, etc., to allow easy refusal of future advertisements for the recipient. Senders are not allowed to use irregular labels in headers.

Furthermore, spamming by using a program or collecting e-mail addresses through technical means are prohibited. The act of sharing, selling, exchanging or providing others with a list of e-mail addresses harvested from Internet bulletin boards is also prohibited. In addition, the Act states that ISPs can deny

services for transmitting information on condition that there is, or will be, intense concern about serious obstruction by large influxes of spam mail. Currently, the opt-out approach is adopted in Korea. However, on 19 October 2003, the Ministry of Information and Communication (MIC) announced that it will introduce an opt-in approach for mobile phone service. As amending the existing law will take time, opt-in will first be implemented via usage agreements between mobile service providers and information service providers. These agreements were to be put in place before the end of 2003. MIC also prohibits sending all advertisement messages during certain hours, for example from 21.00 to 8.00. MIC intends to amend the relevant law in early 2004.

Luxembourg – Opt-in bill in progress

There are currently no rules on unsolicited e-mail, faxes or calls. The government is now trying to introduce new regulation for transposing the Communications Data Protection Directive 2002/58/EC, which, as we have seen, requires opt-in for unsolicited calls, faxes and e-mails.

Mexico – Opt-out

On 11 December 2003, the Mexican Congress approved important reforms and additions to the Federal Law for Consumer Protection. Among those amendments, a few articles were introduced in order to protect personal information and privacy:

- Article 17 - Commercial messages or advertising sent to consumers should indicate the name, address, telephone and, where applicable, the e-mail address of the provider, and of the business that sends the ads on behalf of providers.

  The consumer will be entitled to directly inform specific providers and businesses using its information for marketing or advertising purposes, that s/he does not wish to be bothered at home, or at work, or s/he does not want to receive ads. Likewise, the consumer will be entitled to inform providers or businesses using its information for marketing or advertising purposes, at any moment, that his/her personal data must not be transmitted or shared with third parties, unless that transmission is determined by a judicial authority.

- Article 18 - The *Procuraduría* could develop, where applicable, a consumers' public registry which would list those not wishing their personal data to be used for marketing or advertising purposes. The consumers could notify the *Procuraduría* by letter or e-mail of its inscription request to this registry, which would be at no cost.

- Article 18*bis* - It is forbidden for providers and businesses using consumers' information for marketing or advertising purposes, as well as its clients, to use consumers' information for different purposes from those of marketing or advertising, as well as to send ads to the consumers that have expressly requested not to receive them or that are subscribed to the registry referred to in the previous article. Providers that are the object of advertising are also responsible for the management of consumers' information when such advertising is sent to third parties.

Netherlands – Opt-out, but opt-in bill in progress

The Telecommunications Act of 19 October 1998 is to be replaced at the end of 2003. The new Act requires opt-in for electronic messages for commercial purposes, and soft opt-out for use of contact data

gathered in selling products/services for commercial e-mail. It also requires real identity and address of sender and an opt-out option in messages, as well as prohibits false information in headers and messages.

New Zealand - No regulation

Though New Zealand does not currently have spam legislation, they are actively considering legislative proposals.

Norway - Opt-in

An opt-in approach for e-mail and SMS is implemented by Section 2b of Marketing Control Act which came into force in March 2001. Under the Act, it is prohibited to direct marketing at consumers using methods of telecommunication which permit individual communication, such as electronic mail, text messaging services to mobile telephones, facsimile or automatic calling machines, without the prior consent of the recipient.

Poland - Opt-in

The electronic services law, the Act of 18 July 2002 on Providing Services by Electronic Means, governing online activities including those on the Internet took effect on 10 March 2003. According to the law, service providers have to have buyers' consent for dispatching unsolicited commercial information through electronic communication systems, including e-mail and SMS messages. Otherwise, such operations are classified as unfair competition. This does not apply solely to sending large batches of unsolicited information (spamming), but also to single messages (unsolicited communications).[9]

Portugal - Opt-out, but opt-in bill in progress

An opt-out system is in place for e-mails, while there is no prohibition on unsolicited calls. An opt-in approach is in place for faxes. A wider opt-in draft law is in progress.

Slovak Republic – No regulation

The Slovak Republic currently has no legislation with regard to spam.

Spain - Opt-in

Regarding unsolicited e-mails, calls and other similar electronic communications (such as SMS) used for purposes of direct marketing, an opt-in regime has been adopted for both natural and legal persons. The Law on Services for the Information Society prohibits distribution of mass unsolicited e-mail and stipulates that Internet transactions have the same judicial validity as signed paper agreements. The law was adopted on 27 June 2002.[10] In November 2003, the Telecommunications Act was adopted to implement the EC Directive 2002/58/EC. The Act, an amendment to the Law on Services for the Information Society, introduced an exception to the opt-in model for existing customer relationships.

Sweden - Opt-in regulations in progress

Currently, the Swedish Marketing Act (1995:450) provides two different regimes for unsolicited marketing: opt-in for faxes and automated calling machines; and opt-out for electronic mails and other means of distance marketing. However, on 27 November 2003, a government bill amending the Swedish Marketing Act in order to comply with the provisions of Article 13 of Directive 2002/58/EC was presented to the Parliament. The proposed amendments extend the opt-in regime to electronic mails by incorporating a consent requirement in connection with use of electronic mail in direct marketing to natural persons into the first paragraph of Section 13b of the Swedish Marketing Act. There will be a "soft opt-in" exception from this requirement if there is a previous customer relationship with the recipient, the direct marketing material concerns similar goods or services and the recipient is given a simple, free of charge, means to refuse further e-mail communications. The opt-in rule will only apply when the recipient is a natural person; legal persons will not be covered. "Electronic mail" is broadly defined and includes any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient (e-mail, SMS, MMS, etc.). Furthermore, the government proposes that a prohibition will be incorporated into Section 13c of the Swedish Marketing Act to prevent unsolicited marketing that fails to furnish a valid address to which the recipient can provide notice in the event that he is opposed to receiving further mailings. This provision, however, will be applicable for marketing to all categories of recipients, legal and natural persons. In the event that such marketing is sent out in contravention of this provision, it will be possible to impose a market disruption fee.

The Parliament is expected to make a formal decision in early 2004. If passed, the amendments to the Marketing Act will enter into force on 1 April 2004.

Switzerland - Opt-in bill in progress

The regulations concerning spam, found under Article 45a of the Telecommunication Law *(Loi sur les Telecommunication: LTC)* and Article 3 of the Law against Unfair Competition, are currently being treated in Parliament.[11] They will essentially correspond to the new EU legislation (Directive on data protection on electronic communication networks). Opt-in regulation will thus apply to spam in all forms of messages (*e.g.* phone, e-mail, fax, SMS) and to spam sent to companies as well as consumers. The telecommunication services providers will be obliged to combat spam. In other words, if anyone sends advertisement messages either in bulk or personally without the prior consent of the recipient, or building on a pre-existing business relationship with the recipient, it is considered unfair, and legal action can be taken according to the Law against Unfair Competition. According to the Telecommunications Law, all telecommunications service providers are obliged to use appropriate and reasonable measures to stop spam.

Turkey - No regulation

There is no regulation against spam at the moment. However, discussions are ongoing amongst computer systems administrators and ISP engineers and some experimental work is being carried out, to explore technical solutions, *e.g.* RBLs, etc. to reduce the negative effects of spam on Internet traffic.

United Kingdom – Opt-in

Where e-mail addresses constitute personal data because they contain an individual's name, any processing must be carried out in accordance with the requirements of the Data Protection Act of 1998. This means that any company that continues to process an e-mail address that contains personal data, in

order to send unsolicited marketing communications, after being instructed by the individual to stop, will be in breach of the Act's fair processing requirements.

In March 2003, the UK Department of Trade and Industry introduced new anti-spam regulations, including an opt-in requirement. The law was passed in September 2003 and came into force on 11 December 2003. Under the new law, companies must have explicit permission from e-mail recipients before sending out offers. The law allows individuals to sue companies sending unsolicited e-mail offers. It also requires Web sites to offer consumers the opportunity to reject cookies prior to placing them on users' computers and bans unsolicited text messages. The Information Commissioner will have greater power to follow up complaints. The opt-in rule under the new regulations does not apply to corporate e-mail addresses, which means the law excludes most work addresses from the opt-in requirement.

United States - Opt-out

On 16 December 2003, the United States passed legislation on spam ("CAN-SPAM Act") that, as of 1 January 2004, adopts an opt-out approach to spam. The legislation prohibits false or misleading subject header information and deceptive subject lines. It requires senders of unsolicited commercial e-mail to provide a mechanism to opt-out and requires senders to abide by recipients' requests to opt out. The legislation requires clear and conspicuous disclosure that the message is an advertisement. The senders must include a valid postal address in the e-mail and have a functioning e-mail address. The law also prohibits harvesting of e-mail addresses, dictionary attacks, and spoofing. The legislation also creates new criminal violations. For example, the law makes it a criminal violation to knowingly send unsolicited commercial e-mail with a materially falsified header. Finally, the law requires the FTC to develop a plan and timetable for implementation of a do-not-e-mail registry and report any concerns about such a registry to Congress within 6 months of the enactment of the Act.

ANNEX II. SPAM MATRIX - PART I

	1. Laws / decrees on spam?	2. Title/ effective date of the laws / decrees?	3. Definition / scope of spam?	4. Opt-in, opt-out or none?	5. Any exceptions to opt-in or opt-out?	Comments?
Australia	Yes – Passed by Australian Parliament 2 December 2003	Spam Bill 2003	Unsolicited commercial electronic messages	Opt-in	Government bodies, political parties, religious organisations, charities and charitable institutions, educational institutions	This legislation has a 120-day compliance period and comes into force April 2004.
Austria	Yes	Telecommunications Regulation Act	Bulk e-mails for commercial purposes	Opt-in		
Belgium	Yes	Law on Electronic Commerce, 11/3/2003	Unsolicited commercial electronic mail	Opt-in	Legal person / Pre-existing relationship	
Canada	Applying existing Act	Personal Information Protection & Electronic Documents Act, January 2001	E-mail addresses are considered as personal data	Opt-in		
Czech Republic	Applying existing Act	Act No. 40/1995 Coll. on the regulation of advertising	Unsolicited commercial communications	Opt-in		
Denmark	Yes	Marketing Practices Act	Unsolicited e-mail	Opt-in	Pre-existing relationship	
Finland	Yes	Act on the Protection of Privacy and Data Security in Telecommunications. 1999/565	Unsolicited e-mail, faxes, etc.	Opt-in	Legal persons	New bill is in progress
France	No, opt-in bill is in progress	*Pour la confiance dans l'économie numérique*	Unsolicited e-mail	Opt-in	Registered legal person / Pre-existing relationship	
Germany	No, applying existing Act by court; Opt-in bill is in progress	Bill of an amendment to the Law on unlawful competition *(Gesetz gegen unlauteren Wettbewerb § 7 UWG)*	Unsolicited commercial communication via telephone; automatic calling-machines, fax or electronic mails	Opt-in	In case of a pre-existing relationship: Opt-out	
Greece	Yes		Unsolicited e-mails, calls, faxes for advertising	Opt-in		
Hungary	Yes (Decree)	Gov. Decree Nr. 17/1999 (II. 5.) on distance selling	Means of telecommunication	Opt-out		
Iceland						
Ireland	Yes	SI No. 535 of 2003 European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations, 2003		Opt-in	Pre-existing relationship	

	1. Laws / decrees on spam?	2. Title/ effective date of the laws / decrees?	3. Definition / scope of spam?	4. Opt-in, opt-out or none?	5. Any exceptions to opt-in or opt-out?	Comments?
Italy	Yes (Decree)	Decree No. 171 of 13, May 1998 The "Personal Data Protection Code" (Legislative Decree no. 196 of 30 June 2003), also transposing into Italian legislation Directive 2002/58/EC, enter into force on 1 January 2004	Unsolicited communications for the purposes of direct marketing or sending advertising materials, or else for carrying out surveys or interactive business communication. These include the use of automated calling systems without human intervention, e-mail, facsimile, MMS- or SMS-type messages	Opt-in	Pre-existing relationship	
Japan	Yes	The Law on Regulation of Transmission of Specified Electronic Mail, July 2002; Specific commercial transactions law, July 2002	Unsolicited commercial e-mail	Opt-out		
Korea	Yes	Act on information network and protection, July 2001	Any commercial advertisement via electronic tools	Opt-out		
Luxembourg	No, opt-in bill is in progress					
Mexico	Although there is no specific law on spam, the Federal Law for Consumer Protection covers some e-mail aspects.	Federal Law for Consumer Protection (LFPC) with amendments done in May 2000, and those anticipated in January 2004.	No specific definition in LFPC, but a generally accepted definition for spam is "unsolicited commercial electronic messages".	An opt-out approach is reflected in amendments.		The Legislature is analysing a draft text for regulating data privacy.
Netherlands	Yes	Telecommunications Act, 19 October 1998 (to be replaced end of 2003)	Automated call machines and faxes Other unsolicited calls for commercial purposes	Opt-in Opt-out	Opt-in and opt-out options are to be offered to telecom-subscribers (both legal and natural persons)	Implements EU Directive 2002/58/EC: Opt-in for automated call machines, faxes or electronic messages for commercial purposes; opt-out when other means are used; soft opt-out for use of contact data gathered in selling products/services for commercial e-mail.

	1. Laws / decrees on spam?	2. Title/ effective date of the laws / decrees?	3. Definition / scope of spam?	4. Opt-in, opt-out or none?	5. Any exceptions to opt-in or opt-out?	Comments?
New Zealand	No					Discussion paper being prepared that will discuss the possibility of introducing anti-spam legislation that could complement the legislative measures taken by the EU and Australia.
Norway	Yes	Marketing control Act, March 2001	The conduct of business using methods of telecommunication	Opt-in	If a business relation is previously established, an opt-out is required	
Poland	Yes	Act of 18 July 2002 on Providing Services by Electronic Means	Unsolicited commercial information through electronic communication systems (include single)	Opt-in		
Portugal	No, opt-in bill is in progress			Opt-out / Opt-in draft law in process		
Slovak Republic						
Spain	Yes	Law on Services for the Information Society, June 2002; Telecommunications Act, November 2003	Unsolicited electronic communications	Opt-in	Pre-existing relationship	
Sweden	Yes, electronic mail opt-in regulations in progress	Swedish Marketing Act (1995:450)	Unsolicited marketing by faxes, automated calling machines, electronic mail (SMS, MMS) etc.	Currently opt-in for faxes and automated calling machines / Opt-out for electronic mail and other means of distance marketing	Currently, no	If passed, new opt-in regulations will enter into force on 1 April 2004. Proposed amendments to the Swedish Marketing Act extend the opt-in regime to electronic mail. There will be a “soft opt-in” exception if the marketing concerns similar products or services in an established customer relationship. Legal persons will not be covered by the proposed e-mail opt-in rule.
Switzerland	No, opt-in bill is in progress	Telecommunications law, law against unfair competition	All forms of electronic messages	Opt-in	Pre-existing relationship	
Turkey	No					

	1. Laws / decrees on spam?	2. Title/ effective date of the laws / decrees?	3. Definition / scope of spam?	4. Opt-in, opt-out or none?	5. Any exceptions to opt-in or opt-out?	Comments?
United Kingdom	Yes - opt-in regulations in force from 11 December 2003	Privacy and Electronic Communications (EC Directive) Regulations 2003	Regulations apply to unsolicited commercial e-mail including text messages to mobile phones	Opt-in	Opt-out exemption for existing customer relationships. Legal persons not covered by new e-mail opt-in rules	Implementation of EU Directive on Privacy and Electronic Communications (Directive 2002/58/EC)
United States	Yes	CAN-SPAM Act, 1 January 2004	Unsolicited commercial e-mail	Opt-out		Law covers any "commercial electronic mail message," the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. Definition does not include "transactional or relationship message."

ANNEX II. SPAM MATRIX - PART II

	6. Labelling required?	7. Real ID, address required?	8. Opt-out in messages required?	9. Do-not-spam list required?	10. False information in header and messages prohibited?	11. Use of spamware prohibited?	Comments?
Australia	No	yes	Yes	No	Yes	Yes	SPAM Bill 2003 passed by the Australian Parliament 2 December 2003 and will be enforced with effect April 2004
Austria				Yes (by RTR)			
Belgium		Yes	Yes				
Canada							
Czech Republic							
Denmark	No	Yes	Yes	No	Yes	No	
Finland	Yes	No	Yes	No	Yes	No	New bill is in progress
France	No	Yes	No	No	Yes	Yes	11. loi du 8 janvier 1978
Germany	No	Yes	Yes	No	In header (address): Yes In message : No specific regulation for spam	No	Subject to Parliament approval
Greece							
Hungary							
Iceland							
Ireland							
Italy	No	Yes	Yes	No	Yes	Yes	
Japan	Yes	Yes	Yes	No	Yes	Yes	
Korea	Yes	Yes	Yes	Yes	Yes	Yes	
Luxembourg							
Mexico	No	Yes	No	Yes	Yes	No	
Netherlands	No	Yes	Yes	No	Yes		
New Zealand							Officials are currently reviewing existing legislation to determine if some of these legislative options are already covered.
Norway	Yes	Yes	No	No	Yes, in connection with marketing activities	No	
Poland	Yes	Yes	No	No	Yes	No	
Portugal							

	6. Labelling required?	7. Real ID, address required?	8. Opt-out in messages required?	9. Do-not-spam list required?	10. False information in header and messages prohibited?	11. Use of spamware prohibited?	Comments?
Slovak Republic							
Spain						Yes	
Sweden	Yes, in connection with marketing activities, but no specific regulation for spam	Yes, in connection with marketing activities, but currently no specific regulation for spam	No	Not a statutory requirement	Yes, in connection with marketing activities, but currently no specific regulation for spam	No	New regulations will prohibit unsolicited marketing by electronic mail that fails to furnish a valid address to which the recipient can provide notice in the event that s/he is opposed to receiving further mailings. This prohibition will be applicable for marketing to all categories of recipients, legal and natural persons.
Switzerland	No	Yes	Yes	No	No	No	
Turkey							
United Kingdom	Yes	Yes	Yes	Not a statutory requirement but opt-out registers required under industry codes of practice	Yes	No	Relevant regulations are e-commerce regulations 2002 and privacy regulations 2003
United States	Yes	Yes	Yes	The FTC must report to Congress in June 2004 about establishment of a Do-Not-E-mail registry.	Yes	The law prohibits use of software to harvest e-mail addresses, generate dictionary attacks, and automatically create multiple e-mail accounts to send spam.	

ANNEX III. THE REGULATION ASSOCIATED WITH SPAM IN *EU DIRECTIVE 2002/58/EC OF 12 JULY 2002*

Article 2 - Definitions

(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Unsolicited communications

Article 13.1

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.

Article 13.2

Notwithstanding paragraph 1, 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 products or services, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, 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

Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, 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.

Article 13.4

In any event, the practice of sending electronic mail for purposes of direct marketing 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, shall be prohibited.

There is however an exception for legitimate direct marketing with an existing customer service relationship. Companies will be allowed to send unsolicited commercial mails where they have received the e-mail address directly from the consumer in the context of a purchase and on conditions that:

- the unsolicited e-mail only concerns their own similar products; and
- that the consumer is given the opportunity to object free of charge in an easy manner.

The Directive, however, will only apply to messages sent in Europe.

ANNEX IV. ANTI-SPAM ORGANISATIONS

www.irtf.org/charters/asrg.html (Internet Research Task Force - Anti-Spam Research Group)
www.cauce.org/ (Campaign against Unsolicited Commercial E-mail)
www.euro.cauce.org/ (Euro CAUCE)
www.spamcon.org/
www.mail-abuse.org/
http://mail-abuse.org/swat/
http://spam.abuse.net/
www.junkbusters.com/junke-mail.html
www.spamrecycle.com/
www.junke-mail.org/
www.sputum.com/
www.nanae.org/
www.spamsites.org/
www.spamhaus.org/
www.fmp.com/spam_patrol/
www.natsma.com/
http://sims.net/massacre/
www.gssnet.com/antispam/spam_index.htm
www.stop-spam.org/
www.caspam.org/
www.ripe.net/ripe/wg/anti-spam/
www.cauce.org/orgmember/org_list.shtml
www.caube.org.au/ (CAUCE Australia)
http://cauce.ca/ (CAUCE Canada) (was http://cauce-canada.org/)
http://india.cauce.org/ (CAUCE India)
www.spambr.org/ (Brazilian Spam Fighters)
www.antispam.ru/ (Russian anti-spam site)
http://nospam.spb.ru/ (Russian)
www.aui.es/contraelspam/ (Spanish Association of Internet Users)
www.fabel.dk/ (Danish site)
www.spam.org.tr/ (Turkish anti-spam site)
www.antispam-argentina.8m.net/ (Argentine anti-spam site)
www.spamstop.net/ (Japanese)
www.cauce.nl/ (Dutch)
www.ihatespam.biz/ (Korean)
www.iajapan.org/hotline/ (Japanese)
www.spamstop.net/ (Japanese)
www.nospamware.it/ (Italian)
www.uzice.net/yasi/ (Yugoslav Anti-Spam Initiative)

Source: SpamCon Foundation, 2003.

NOTES

1. OECD (2003), *OECD Communications Outlook 2003,* OECD, Paris.

2. See "Internet Indicators: Hosts, Users and Number of PCs", International Telecommunication Union, www.itu.int/ITU-D/ict/statistics/at_glance/Internet02.pdf, accessed 9 January 2004.

3. See "Population explosion", by CyberAtlas staff, 14 March 2003, http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_151151,00.html, accessed 9 January 2004.

4. See Markoff, John (2003), "Start Up Finds Technology Slump Works in its Favor", 24 March 2003, www.nytimes.com/2003/03/24/technology/24PHIL.html, accessed 9 January 2004.

5. See Industry Canada (2003), "E-mail Marketing: Consumer Choices and Business Opportunities", Discussion Paper, January, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00189e.html, accessed 22 January 2004.

6. According to a survey of consumers conducted in 2002 for Symantec Corp. by InsightExpress, some interesting findings include:

   - 37 % of respondents receive more than 100 spam e-mails each week at home and work.
   - 63 % receive more than 50 spam messages weekly at home and work.
   - 69 % of respondents agreed or strongly agreed that spam is generally harmful to e-mail users. MessageLabs reports one virus interception in every 212 e-mails in 2002 — up from one out of 380 in 2001 — with "Klez" as the number one virus of 2002, with five million copies captured.
   - 77 % of respondents with children under the age of 18 noted that they are concerned or very concerned about their children reading spam.
   - 38 % indicated that pornographic or otherwise inappropriate spam content was considered their primary concern. The "Nigerian Scam" alone has spread worldwide, and MessageLabs expects the operation to gross over two billion dollars in 2003, becoming the second largest industry in the country, if e-mail users continue to be deceived.
   - 84 % agreed or strongly agreed that spam places a burden on their individual time.
   - 36 % responded that it takes too much time to delete or unsubscribe to spam messages.
   - 42 % of respondents didn't use a spam filter.
   - 18 % of respondents indicated that spam takes up limited computer and e-mail resources.

   See Greenspan, Robyn and Brian Morrissey (2002), "Spam Expected to Outnumber Non-Spam", Jupitermedia Corporation, 12 December, http://cyberatlas.internet.com/big_picture/applications/article/0,,1323,1301_1555831,00.html, accessed 9 January 2004.

7. The Radicati Group (2003), "Anti-spam Market Trends, 2003-2007", www.radicati.com/cgi-local/brochure.pl?pub_id=202&subscr=&back_link=/single_report/, accessed 8 December 2003.

8. It is an American trademark for a "spicy ham" product in a can. It is used in our context because of a British Monty Python humoristic show picturing a man and his wife in a restaurant in which the waitress proposes spam with every dish even though the customer does not want any.

9. See EC (2001), "Unsolicited Commercial Communications and Data Protection", January, http://europa.eu.int/comm/internal_market/ privacy/docs/studies/spamsum_en.pdf, accessed 9 January 2004.

10. See www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf, accessed 9 January 2004.

11. This list of characteristics is not exhaustive.

12 . See Association for Interactive Marketing (2002), "Survey on the Commercial Use of E-mail", www.interactivehq.org/councils/CRE/valuesurvey.asp, accessed 9 January 2004.

13. See Cerf, Vinton and Orson Swindle (2002), "Spam: Can It Be Stopped?" 18 June, www.gip.org/publications/papers/Spam061802.asp, accessed 9 January 2004.

14. See Mailshell (2003), "SpamCatcher Attitude Survey", released on 1 May at the US Federal Trade Commission (FTC) Spam Forum.

15. *Wall Street Journal*, 13 November 2002.

16. A report from the US FTC shows that Web pages, newsgroups and chat groups are more vulnerable to the spammers than other sources. According to the report, investigators seeded 175 different locations on the Internet with 250 new, undercover e-mail addresses to find out which fields spammers consider most fertile for harvesting. The locations included Web pages, newsgroups, chat rooms, message boards, and online directories for Web pages, instant message users, domain names, resumes, and dating services. During the six weeks after the postings, the accounts received 3 349 spam e-mails. The investigators found that:

- 86 % of the addresses posted to Web pages and newsgroups received spam.
- Chat rooms are virtual magnets for harvesting software.

See FTC (2002), "E-mail Address Harvesting: How Spammers Reap What You Sow", November, www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm, accessed 9 January 2004.

17. According to Spamhaus, spammers have conducted a massive five-month-long dictionary attack against the mail servers of Hotmail and MSN to harvest the e-mail addresses of millions of Hotmail and MSN users. Spamhaus recommends that users of ISPs use a long username with random characters to prevent their addresses being harvested. See Spamhaus (2003), "Spammers Grab MSN Hotmail Addresses", 5 January, www.spamhaus.org/news.lasso?article=6 , accessed 9 January 2004.

18. There are two types of bulk e-mail services available on the market. While spam campaign hosting companies offer the various range of services required to organise a spamming campaign, the e-mail address brokers supply many lists or e-mail addresses. In response to the anti-spammers, the e-mail address brokers also offer the options for removal of opt-in lists in which there are address of known anti- spam activists, and of the .gov, .mil and .edu domains.

See Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, p. 33, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

19. See www.spamhaus.org/sbl/sbl-rationale.html , accessed 9 January 2004.

20. See www.spamhaus.org/sbl/sbl-rationale.html , accessed 9 January 2004.

21. See Solomon, Melissa (2002), "Spam Wars", *Computerworld Inc.*, 11 November, http://computerworld.com/softwaretopics/software/groupware/story/0,10801,75737,00.html , accessed 9 January 2004.

22. See Mobile Marketing Association (2001), "Wireless Advertising Association Formally Adopts Standards for WAP, SMS and PDA Advertising", Press Release, 30 July, www.mmaglobal.com/press/archived_news/standards_for_WAP.html , accessed 9 January 2004.

23. See Olsen, Stefanie (2003), "Net Users Want Law to Can Spam", Oaxaca Lending Library, 3 Januarywww.oaxlib.org/spamcost.html , accessed 9 January 2004.

24. See Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

25. See Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, pp. 66-67, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

You can see how to calculate the cost in this report in the below:

"Assuming that an average Internet user paying a flat-rate fee of EUR 12 a month for 10 hours connection time (including telephone calls) and using standard equipment (without a broadband connection) can 67download messages at a rate of about 180 K/bits per minute, the cost of downloading just 15 or so messages a day totalling between 500 and 800 K/bits in size could be as high as EUR 30 a year. If this is multiplied by the number of Internet users in a given country, the overall cost becomes very substantial indeed. Or on a world scale, assuming a worldwide online

community of 400 million, the global cost of downloading advertising messages using current technology may be conservatively estimated at EUR 10 billion – and that is just the portion of the cost borne by the Web surfers themselves."

26. See Greenspan, Robyn and Brian Morrissey (2002), "Spam Expected to Outnumber Non-Spam", Jupitermedia Corporation, 12 December, http://cyberatlas.internet.com/big_picture/applications/article/0,,1323,1301_1555831,00.html, accessed 9 January 2004.

27. See Brightmail (2003), "The State of Spam – Impact & Solutions", January, p. 7, www.brightmail.com/press-vpk.html , accessed 9 January 2004.

28. The Radicati Group (2003), "Anti-spam Market Trends, 2003-2007", www.radicati.com/cgi-local/brochure.pl?pub_id=202&subscr=&back_link=/single_report/, accessed 8 December 2003.

29. See Morrissey, Brian (2003), "Spam Cost Corporate America $9B in 2002", Jupitermedia Corporation, 7 January, http://cyberatlas.internet.com/big_picture/applications/article/0,,1301_1565721,00.html , accessed 9 January 2004.

30. See Krim, Jonathan (2003), "Spam's Cost To Business Escalates", *Washington Post*, 13 March, http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12, accessed 9 January 2004.

31. See NOIE (National Office for the Information Economy) (2002), "The Spam Problem and How it Can be Countered – An Interim Report by NOIE", Australia, 1 August, p. 11.

32. See Brightmail (2003), "The State of Spam – Impact and Solutions", January, p. 7, www.brightmail.com/press-vpk.html , accessed 9 January 2004.

33. See Court, Randolph H. and Robert D. Atkinson (1999), "How to Can Spam", 1 November, www.ppionline.org/ndol/print.cfm?contentid=1349 , accessed 9 January 2004.

34. See FTC (2003), "False Claims in Spam", Division of Marketing Practices, 30 April, www.ftc.gov/reports/spam/030429spamreport.pdf, accessed 9 January 2004.

35. From the responses of European ISP federations it transpires that even today over 40 % of mail servers in operation in Europe still have a relay function and are therefore unable to prevent spam being relayed to all the e-mail addresses managed by them.

See Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, p. 98, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

36. See Brian D. Westby, FTC V., FTC, File No. 032 3030, filed 15 April 2003, www.ftc.gov/opa/2003/04/westby.htm, accessed 19 January 2004.

37. In January 2003, Brightmail measured 5% of spam to be scams, defined as "e-mail attacks recognised as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender." A letter from someone claiming to be a Nigerian citizen prompts the recipient to send a sum of money in order to help free up a bank account holding millions of dollars. While this scam seems ludicrous to some, its success has kept it circulating through millions of inboxes.

38. See "Public Awareness Advisory Regarding "4-1-9" or "Advance Fee Fraud Schemes", www.secretservice.gov/alert419.shtml , accessed 9 January 2004.

39. In March 2003, the messages asked PayPal subscribers, users of eBay's online payments service, to submit bank and credit card details. This bogus spam messages posing as legitimate messages from eBay and PayPal included a PayPal logo, links to PayPal's site and official-looking fine-print which is appeared particularly convincing. The e-mails told recipients that their PayPal accounts have been randomly selected for maintenance and placed on "Limited Access" status. The message, which appears to come from info@paypal.com, instructs the account holder to enter credit card and bank account numbers in an online form embedded in the e-mail. Spammers had been arrested and given jail time because they had not delivered the promised product.

40. According to the white paper of Brightmail co. in 2003, 18% of spam is now touting pornography. Naked women performing oral sex with guns pressed to their heads, naked women with large dogs clutching their backs, naked women in pigtails pretending to be daughters having sex with fathers. These are some of the explicit images that have started slipping into inboxes lately as spamsters try to drive traffic to a growing number of sites featuring rape, bestiality and incest pornography.

41. See Brightmail (2003), "The State of Spam – Impact and Solutions", White Paper, Document Version 1.0, January, p. 6, www.brightmail.com/press-vpk.html , accessed 9 January 2004.

42. See *PC World* (2003), "Sobig May Be Working for Spammers", 29 August, www.pcworld.com/news/article/0,aid,112261,00.asp , accessed 9 January 2004.

43. According to the FTC, one defendant used deceptive spam, including unauthorised use of logos of well-known financial institutions including Radian Bank, Prudential, and Fannie Mae, to induce victims to disclose sensitive financial information such as income, mortgage balances, and home values in November 2002. The spammers purported to offer consumers competitive financing and refinancing loans. The defendants also allegedly forged e-mail headers - a technique known as "spoofing," - so that any undeliverable messages went to e-mail addresses unaffiliated with the defendants.

See FTC (2002), "Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams", 13 November, www.ftc.gov/opa/2002/11/netforce.htm , accessed 9 January 2004.

44. The guidelines are available at www.oecd.org/dataoecd/5/34/1824782.pdf.

45. For example, the Australian government has applied the following relevant existing civil and criminal laws to deter or punish the sending of electronic communications in Australia:

- Breach the National Privacy Principles in the Privacy Act.
- Breach the prohibitions against promoting x-rated content on Web sites or most forms of interactive gambling.
- Breach fair trading, anti-fraud and investor protection provisions in the Trade Practices Act and the Corporations Law.
- Breach the Cybercrime Act through hacking and possibly spoofing.

46. Where e-mail addresses do not contain an individual's name they may not be regarded as personal information under the Privacy Act and therefore not covered by it. In this case, the new law or modification of current related law may be considered.

47. Some organisations such as the Global E-mail Marketing Association (GEMA) are worried about this kind of regulation because of the death threats they have received. GEMA says that many of its members are small businesses and work out of a home office and in such cases disclosure of their address would endanger both them and their families. So, they believes that the legislative intent can be satisfied if the marketer include either its address or telephone number. See "Statement of Marie Monroe, President of GEMA", Press Release, FTC Spam Forum, 2 May 2003.

48. GEMA worries about the deceptive and unfair business practices and recommends that the regulation authority such as the FTC monitor the marketplace to ensure that ISPs do not use their market power to eliminate competitors in the e-mail marketing space.

49. The GEMA argues that Web crawlers, software programs used to cull e-mail address posted on public Internet sites should not be prohibited as proposed in current legislation. It says that there is nothing pernicious about crawlers and these programs do not involve hacking into any computers or databases. See "Statement of Marie Monroe, President of GEMA", Press Release, FTC Spam Forum, 2 May 2003.

On the other hand, the Direct Marketing Association (DMA) opposes surreptitious harvesting and 'dictionary attacks' of e-mail addresses. According to the DMA, both practices constitute abuses of the right to send e-mail legitimately and could ultimately undercut e-mail as a valuable business communications tool. See "The DMA opposes surreptitious harvesting and 'dictionary attacks' of e-mail addresses" released by DMA at the FTC Spam Forum, 30 April 2003.

50. Member states were required to implement the new rules in national legislation by 31 October 2003. The European Commission has launched infringement proceedings against a number of member states that failed to notify those transposition measures.

51. For example, see Directive 2000/31/EC of 8 June 2000 on electronic commerce which includes provisions for transparency in relation to e-mail marketing, notably requiring that commercial communications must be identifiable as such.

52. See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

53 . The FTC has invited consumers to forward their spam to a special address (uce@ftc.gov), and has built a spam database that serves as a resource for investigators. Consumers forward spam messages to the FTC at a rate of approximately 105 000 e-mails a day, as of May 2002.

54. See FTC (2003), "False Claims in Spam", Division of Marketing Practices, 30 April, www.ftc.gov/reports/spam/030429spamreport.pdf, accessed 9 January 2004.

55. See ePrivacy Group (2003), "2003 Consumer Spam Study", July, www.eprivacygroup.net/spamstudy , accessed 9 January 2004.

56. Spamhaus (//spamhouse.org) tracks the Internet's worst spammers, known Spam Gangs and Spam Support Services, and works with ISPs and law enforcement agencies to identify and remove persistent spammers from the Internet. Spamhaus provides users with "The Spamhaus Block List (SBL)" which is a free real-time DNS-based database of IP addresses of verified spammers, spam gangs and spam services.

57. CAUCE actively participates in the submission of legislative bills intended to limit or prohibit unsolicited commercial e-mail. Euro-CAUCE launched a petition against "spamming" to be addressed to members of the European and national Parliaments.

58. See www.tacd.org

59. In the United States, ISPs have organised a network of voluntary administrators known as The Mail Abuse Prevention System which operates the Realtime Blackhole List (RBL). This list is an instrument of mass boycott used by the ISPs' system administrators to ostracize IP addresses and domain names of spammers. Refer to Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, http://europa.eu.int/comm/internal_market/ en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

60. For example, with Acceptable Usage Policy (AUP), "Telstra BigPond Direct", the largest backbone ISP in Australia, makes it clear that spamming is unacceptable and that they will terminate service to spamming customers.

"Telstra Bigpond's Terms of Use Regarding Spam:

2.1 You must not:

- Use telstra.com to send unsolicited electronic mail messages to anyone.
- To make any fraudulent or speculative enquiries, bookings, reservations or requests using telstra.com.
- Use another's name, username or password without permission.
- Post, or transmit via telstra.com, any obscene, indecent, inflammatory or pornographic material or material that could give rise to civil or criminal proceedings.
- Tamper with, hinder the operation of or make unauthorised modifications to telstra.com.
- Knowingly transmit any virus or other disabling feature to telstra.com."

61. See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

62. See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

See NOIE (2002), "The Spam Problem and How it Can be Countered – an Interim Report by NOIE", Australia, 1 August.

In Australia, the Internet Industry Association code of practice(version 5) makes the following restrictions on spam in section 10:

- IIA members and code subscribers must not spam, and must not encourage spam, with exceptions in the case of pre-existing relationships.
- IIA members and code subscribers who do use acquaintance spam must provide recipients with the capability to opt-out, and must include opt-out instructions in the spam.
- IIA members and code subscribers must not send even acquaintance spam containing prohibited content.

- IIA member and code subscriber Internet Service Providers should have an Acceptable Use Policy that prohibits spam, and further prohibits services that depend on spam.

- ISPs should have a working contact address for spam complaints - that is, an "abuse@" e-mail address.
- ISPs should install relay protection on their mail servers, to prevent spammers from using the relay to evade detection or penalty.

63. Within the online stamp system, the bulk commercial e-mail senders who want to send more than 1 000 mails per day have to pay for them and should register their real name in advance with Daum. If the bulk e-mail sender didn't register before, its e-mail will be blocked by Daum. Even though the sender paid already, if the recipients of the mail responded through recipient's votes that the e-mail is not commercial but informative and valuable, then Daum refunds the money to the sender differentially according to the informative ratio in its pre-set refund table (Daum reward point system). Daum, of course, sells the on-line stamp and operates registrants on line, or its Web site. Daum also introduced the "spam claim index" in which there are 4 level indexes, that is, "clean", "attention", "warning", "restriction". "Restriction" levelled-registered IP, which got a most spam claims, might be limited for bulk e-mailing.

    According to the public poll done by Daum in 2002, the responses that the spam decreased after the online stamp system was 76.6%, the responses that there is no difference was 23.4%, and the percentage of people who are pro to the system is 83.5%. Even though the e-mail senders asked the users of Daum to change e-mail address to other ESPs, the percentage of people who responded that they would continuously use Daum mail service as primary was 88.4%. With regard to online stamp of Daum, see http://onlinestamp.daum.net/intro.jsp, http://onlinestamp.daum.net/focus/focus2.jsp, , accessed 9 January 2004.

64. See Internet Industry Association, "National Spam Initiative", www.iia.net.au/nospam , accessed 9 January 2004.

65. "Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves".

66. See Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, p. 91, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

67. See http://preference.the-dma.org/products/empssubscription.shtml, accessed 9 January 2004.

68. See www.tpsonline.org.uk/, accessed 9 January 2004.

69. See DMA (2002), "Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary", January, www.the-dma.org/guidelines/onlineguidelines.shtml#2 , accessed 9 January 2004.

70. Under this code, consumers who are solicited must be given the opportunity of "opting-out" of any further communication from the marketer. A marketer who fails to live up to the CMA code is expelled from the Association.

71. See www.networkadvertising.org

72. CDT suggested some ways that people can hide from spammers, including:

    - Disguise e-mail posted to a public place or do not post their Web addresses in public directories.
    - Pay special attention to check boxes that ask for the right to share their e-mail address.
    - Use multiple e-mail addresses.
    - Use a filter.
    - Don't use a short e-mail address.

    See CDT (2003), "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report", March, www.cdt.org/speech/spam/030319spamreport.shtml, accessed 9 January 2004.

73. Being developed by ePrivacy Group, these messages contain trust stamps, clearly visible in the upper-right of the e-mail, which let recipients verify, in real-time, the authenticity of the sender, the integrity of the e-mail, and the sender's compliance with e-mail privacy and best practice principles, based on industry and advocate consensus.

74. See www.ecommerce.treasury.gov.au

75. See www.msn.co.uk/spambuster.

76. See ePrivacy Group (2003), "Trusted E-mail Open Standard", White Paper, May, pp. 2-3.

77. See Solomon, Melissa (2002), "Spam Wars", *Computerworld Inc.*, 11 November, http://computerworld.com/softwaretopics/software/groupware/story/0,10801,75737,00.html , accessed 9 January 2004.

78. One of these kinds of solutions is "Trusted E-mail Open Standard", proposed by ePrivacy group at the FTC Spam Forum, 2 May 2003, which allows senders of e-mail to make verifiable assertions in the header of a message regarding their identity and the content of the message. This was endorsed by CAUCE, SpamCon Foundation and CAUCE Canada. At the FTC Forum, participants including marketers, ISPs, consumer advocates and technology companies agree the necessity of a consensus-based effort to deploy tools that e-mail senders can use to add verifiability to their messages. The Trusted E-mail Oversight Board was proposed to create programs that certify e-mail based on a set of standards that program participants then agree to meet. See ePrivacy Group (2003), "Trusted E-mail Open Standard", White Paper, May, and http://eprivacygroup.net/toes

79. Heuristic analysis software looks for invalid message IDs, bugs, and other spam traits and develops a numerical score for each incoming mail. If the score hits a designated limit, the e-mail is blocked.

80. See Berlind, David (2003), "First Industry-wide Antispam Conference Shows Promise", Oaxaca Lending Library, 27 February, www.oaxlib.org/v-37.html, accessed 9 January 2004.

81. See www.irtf.org/charters/asrg.html, accessed 9 January 2004.

82. See http://www.isipp.com/news.html, accessed 9 January 2004.

83. In the United Kingdom, an MP (Member of Parliament) called for the government to rethink of the filtering system in February 2003, which was intended to free MPs inboxes from the menace of spam and pornography but had also been blocking legitimate debate about the Sexual Offences Bill. See BBC News (2003), "MPs Call for Anti-spam Rethink", 10 February, http://news.bbc.co.uk/1/hi/technology/2737221.stm, accessed 9 January 2004.

84. The AC Nielsen consult survey of Australian ISPs found that, of the five largest ISPs, only one filtered for spam before their mail servers forwarded mail to customers. One of the remaining four said it is active in encouraging its customers to employ filter products (provided through the ISP at a discounted price). Of the other smaller Australian ISPs, most employed filters before forwarding mail, but many did not filter for all spam.

    See NOIE (2002), "The Spam Problem and How it Can be Countered – an Interim Report by NOIE", Australia, 1 August, p. 23.

ANNEX I NOTES

1. See Gauthronet, Serge and Etienne Drouard (2001), "Unsolicited Commercial Communications and Data Protection", European Commission, January, p. 75, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf, accessed 9 January 2004.

2. See EC (2003), "Overview of Implementation in the Member States" of the "Eighth Report from the Commission on the Implementation of the Telecommunications Regulatory Package", Annex 3, European Telecoms Regulation and Markets 2002, 3 December, http://europa.eu.int/information_society/topics/telecoms/implementation/annual_report/8threport/index_en.htm, accessed 9 January 2004.

3. See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

4. See Industry Canada (1999), "Internet and Bulk Unsolicited Electronic Mail (SPAM) Policy", July, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html, accessed 9 January 2004.

5. For example, the government tries to adapt the regulation of the sending of unsolicited communications (spamming) under Art. 7 of the Directive (sender identification by the recipient, introduction of registers of persons opting out of spam, and duty of sender to consult those registers) as the Act No. 40/1995 Coll., on the regulation of advertising, is too general on this issue (provides for no penalty) and its wording is too restrictive at the same time.

6. In addition, the bill also called for Internet site hosts to be responsible for a "minimum of surveillance" of their pages, to prevent the diffusion of messages or images of racism, paedophilia and crimes against humanity. E-commerce would also be tightened up, with those offering on-line sales handed "global responsibility" for those sales.

7. See Budai, Judit (2000), "Overview of Electronic Commerce", International Law Office Internet Publication, September, www.szecskay.hu/publikaciok/jbuy010.pdf, accessed 9 January 2004.

8. See Cramer, Evan (2002), "The Future of Wireless Spam", *Duke Law and Technology Review*, Rev. 0021, www.law.duke.edu/journals/dltr/articles/2002dltr0021.html, accessed 9 January 2004.

9. See "Spam Slammed", *The Warsaw Voice News*, 13 March 2003, www.warsawvoice.pl/view/1593, accessed 9 January 2004.

10. Opponents of Spain's new e-commerce law requiring ISPs to keep tabs on users have vowed to challenge it in court as a violation of constitutional rights. See Socolovsky, Jerome (2002), "Spain's New E-Commerce Law Worries Privacy Advocates", Associated Press, 28 June.

11. See *"Projet de loi sur les télécommunications"*, Article 45a and Annex (*Modification du droit en vigueur*), www.bakom.ch/imperia/md/content/francais/telecomdienste/principesetconsultations/consultations/ProjetdeloiLTC.pdf, accessed 9 January 2004.

    Also see Explanations under Sections 2.1.7 (Art. 45a LTC), 2.2.1 (Art. 3 LCD), *"Message relative à la modification de la loi sur les télécommunications"*, www.bakom.ch/imperia/md/content/francais/telecomdienste/principesetconsultations/consultations/MessageLTC.pdf, accessed 9 January 2004.