ITU WSIS THEMATIC MEETING ON COUNTERING SPAM

SPAM IN THE INFORMATION SOCIETY: BUILDING FRAMEWORKS FOR INTERNATIONAL COOPERATION



This paper was prepared by Claudia Sarrocco, Policy Analyst, International Telecommunication Union, for the ITU World Summit on the Information Society (WSIS) Thematic Meeting on Countering Spam. The annex was compiled by Cristina Bueti, ITU. This meeting was organized under the ITU New Initiatives Programme of the Office of the Secretary-General of the ITU.

The meeting project was jointly managed by Robert Shaw (Robert.shaw@itu.int) and Claudia Sarrocco (Claudia.sarrocco@itu.int) both of the Strategy and Policy Unit (SPU), and the series is organized under the overall responsibility of Tim Kelly, Head, SPU. The papers prepared for the meeting, as well as further information on the New Initiatives Programme, can be found at www.itu.int/ni.

The views expressed in this paper are those of the author and do not necessarily represent those of ITU or its membership.

Table of contents

1	Intro	duction4		
2	Span	n basics	4	
	2.1	What is spam?	6	
		2.1.1 Wireless spam	7	
		2.1.2 Spam over instant messaging—or "Spim"	9	
	2.2	Spam, viruses and fraud	9	
	2.3	The impact of spam	11	
3	Tech	Technical solutions and legal environment: cross-border issues		
	3.1	Technical solutions	12	
	3.2	Legislation	14	
		3.2.1 Spam laws	14	
		3.2.2 Non-specific spam laws	16	
	3.3	Enforcement	17	
4	Inter	national initiatives in the field of spam	18	
5	Conc	clusions: Act locally, think globally	21	
	5.1	The role of users	21	
	5.2	The role of industry		
	5.3	The role of governments		
	5.4	A final word		
Anne	<u>x I</u>			

1 Introduction

As the Internet becomes increasingly accessible from all parts of the world, recent studies have revealed that more than half of all e-mail communications are constituted by spam messages. Spam activities are now spreading to mobile phone multi-media messaging services and instant messaging services. Spam is not only growing, but also evolving in its nature: the emergence of fraudulent spam raises issues for individuals and businesses alike, including invasion of privacy, exposure to illegal or offensive content, misleading trade practices and expense, menacing the effectiveness of electronic communication and legitimate online business. Spam that carries dangerous computer viruses also constitutes a threat to security of the information infrastructure.

As is often stated, there is no "silver bullet" solution to the problem. Technical solutions may be capable of eliminating a good percentage of spam, but only after it has been sent. Industry self-regulation, in terms of policies and guidelines to educate and monitor the practices of end-users, can also have some effect in stemming the tide of spam. However, there is a clear need to prevent spam from being sent in the first place. Legislation is seen as playing a crucial role in stopping spam at the source. In the United States and the European Union (EU), legislative measures have recently been updated and/or implemented specifically to combat spam. The initial impact of such legislation, however, appears to be moderate and enforcement mechanisms are insufficient. Furthermore, it is apparent that spam is a cross-border issue that requires international solutions.

During the Geneva phase of the World Summit on the Information Society (WSIS) in December 2003, the issue of spam—or unsolicited commercial communications—was discussed extensively, in particular in relation to the need for a secure Internet environment, in which the potential of new communication technologies can be fully exploited by users.² Summit participants recognized that spam is a "significant and growing problem for users, networks and the Internet as a whole" (WSIS Declaration, paragraph 37). During the Summit, the issue could not be discussed in further detail. However participants agreed that, in order to build confidence and security in the use of ICTs, there is a need to "take appropriate action at national and international levels" (WSIS Plan of Action, paragraph C5, d).³

This concept was supported not only during the Summit, but also during various meetings at national, regional and international levels that have dealt with the issue of spam.⁴ The WSIS Plan of Action reinforces these views and calls for further action by all stakeholders.

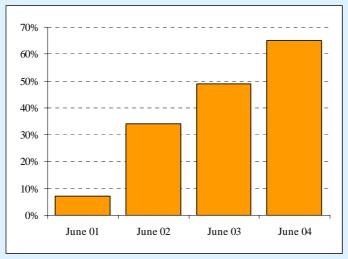
2 Spam basics

The problem of unsolicited commercial e-mail or spam, as it is usually known, has been growing during the last ten years. An analysis of the current statistics on unsolicited commercial e-mail provides an overview of the problem and serves as a starting point in identifying some of the issues associated with this phenomenon, its impact and the possible solutions (Figures 1 and 2).

According to MessageLabs, a US consultancy firm, spam now accounts for around 76 per cent of all e-mail traffic.⁵ The European Commission (EC) estimates the cost of spam to Internet users worldwide to be around 10 billion Euros per year, and a recent study has estimated the loss of productivity due to spam messages at USD 1'930 per employee, per annum.⁶ This does not include the cost of damage caused by viruses, consumer fraud and identity theft; crimes that are increasingly perpetrated through unsolicited e-mail sent to users.⁷ Spam has clearly become a new security threat. The major "spammer" source countries are currently the United States, followed by China, South Korea, Brazil and Canada.⁸

Figure 1: Spam growth worldwide from June 2001 to June 2004

Spam as a percentage of global e-mail, worldwide.



Source: Brightmail statistics, online at http://www.brightmail.com/spamstats.html,

There is little mystery to the burgeoning expansion of spamming activity: if it has become such a widespread problem, it is because it is financially profitable. This is due to the low start-up costs for spammers, and the marginal cost of sending spam, which is virtually zero (it has been estimated that it costs, on average, 0.05 US cents to send each e-mail). Furthermore, the basic Internet architecture, based on Simple Mail Transfer Protocol (SMTP), is intrinsically insecure, allowing spammers to operate anonymously and to evade law enforcement. Last, but not least, despite widespread consumer awareness about the risks involved in responding to unsolicited e-mail marketing offers over the Internet, it is estimated that about one third of users click on a link provided in a spam e-mail, and about 7 per cent respond and lose money to spammers, proving that it can be an effective marketing tool. In

While unsolicited commercial messages were quickly recognized as a problem, it has typically been deemed beyond the realms of government interference as it has been considered exclusively the role of the Internet community to deal with Internet matters. This has led to the elaboration of codes of conduct and the emergence of "netiquette", a set of behavioural norms of the Internet. Netiquette is typically based on "moral" pressure, where the loss of reputation and the contempt of other members was enough to isolate eventual violators and act as a deterrent. However, it only really worked in the context of a relatively small user community.

Self-regulation reached its limits with the mass-diffusion of electronic communications. Users no longer have the feeling of belonging to a community, and simply use the Internet as a tool to communicate for professional, commercial or personal reasons. Furthermore, the majority of spam advertising proposes goods or services that are of dubious quality—pornographic material, gambling, etc.—the kind of marketing sources and products against which social pressure tends to be ineffective.

A further step to regulate this phenomenon was taken by the most directly affected entities, Internet service providers (ISPs), which can undertake measures to regulate the utilization of their resources by their clients through an appropriate clause in their contractual user policy, by banning, for example, the sending of bulk mail over their networks. Furthermore, attempts are being made to standardize business practices or at least to harmonize ISPs' approach in countering spam.¹² This constitutes indeed a first step to curb spam, but this alone will not be sufficient. As long as companies are allowed to market software which facilitates spammers to conceal or forge mail-origin data, or to facilitate the unauthorized use of resources (such as using third party mail server relays), the problem of unsolicited e-mail will continue to grow at the expense of ISPs and consumers.

ISPs have also deployed filtering solutions to block spam before it reaches their users' inboxes: AOL has reported that it blocks over 2 billion e-mails a day. Similarly, Hotmail and MSN servers block about 2.4 billion messages a day. Blocking is, however, insufficient to combat the problem, and advanced filtering techniques are soon outpaced by new methods of sending spam.

Some groups, such as the Coalition Against Unsolicited Commercial Email (CAUCE), offer legal and technical advice on how to combat spam and engage in lobbying activities, while the Mail Abuse Prevention System (MAPS) maintains a list of servers that allow spam to originate from their systems along with the organization responsible for sending spam. Spamhaus, with its Spamhaus Block List (SBL) follows similar procedures. ISPs worldwide subscribe to these lists and block all e-mail from servers included on the blacklist. The utilization of such lists, however, is controversial. First, inclusion on a blacklist is based on criteria that are entirely dependent on the definition that is given of illegitimate spam. This leaves a significant margin of uncertainty as to the reliability of the lists. Is

A number of proposals have been put forward by the Direct Marketing Association, ¹⁶ which has adopted a code of conduct for their members. However, even if a few larger enterprises agree to adhere to the DMA's code, the large majority of generators of unsolicited e-mails does not feel bound by "legitimate" marketing procedures and have no incentive to follow such policies.

In the late nineties, governments began to intervene in the field by establishing appropriate legislation to deal with the proliferation of spam.¹⁷ The first governmental initiative to implement such legislation was taken in the State of Nevada, in the United States of America. Since then, a number of countries have established their own anti-spam legislation. The United States has recently enacted a federal anti-spam law, the CAN-SPAM act,¹⁸ while the European Union—after having already issued several Directives that deal with privacy and consumer protection in the electronic environment—issued its Directive 2002/58¹⁹ dealing specifically with unsolicited electronic communications. This legislation is currently being implemented in EU member countries. In Australia, an anti-spam law came into effect at the beginning of 2004, and the Republic of Korea relies heavily on legislation and effective enforcement to deal with the growing amount of spam affecting the country.²⁰

Notwithstanding the different views and approaches, all players agree that there is no easy solution to the spam problem, and that a multi-pronged and cooperative approach is necessary. As stated by an Internet group addressing the problem of spam, "spam is the number one problem of the Internet and it affects all of us [...]. The solution is not technical, not legal, not standardization, but a combination of all of them and it requires cooperation." Cooperation, between public and private stakeholders, and at the international level, is a key element for a comprehensive and effective strategy against spam.

2.1 What is spam?

The term "spam" was applied for the first time to articles posted to online message boards, which were of no relevance to the their discussions and violated their forum policies. Such articles were sent to several newsgroups, and quickly became a nuisance to other users.²² The term was then applied to describe junk email messages, usually advertisements for product and services often of a dubious nature. Today the term is used as a synonym for unsolicited commercial e-mail.

Several stakeholders have given definitions of spam, and although there are common points, there is still no universally accepted definition. Broadly speaking, spam includes all electronic messages that are unsolicited or unwanted, sent to a large number of users (bulk)²³ without regard to the identity of the individual user, usually having commercial purposes, and that can include viruses that propagate via e-mail, or fraud and scam mechanisms. The *Commission Nationale de L'Informatique et des Libertés* (CNIL), an independent French authority dealing with data protection, defines spam as:

"The practice of sending unsolicited e-mails, most frequently of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact, and whose e-mail address may be found in a public place on the Internet, such as newsgroups, mailing lists, directory or website." ²⁴

From a technological point of view, spam is not limited to unsolicited e-mail messages. The European Union in its Directive 2002/58 took a technology-neutral approach, and used the term "unsolicited commercial communications" or "electronic mail for the purposes of direct marketing". "Electronic mail" includes "any

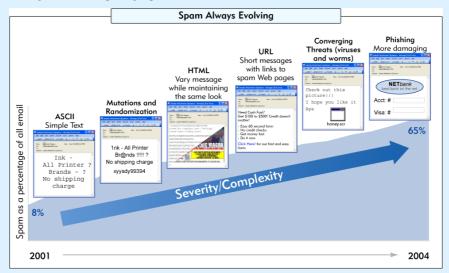
text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient". This is in an attempt to regulate spam sent via e-mail, but also covers spam sent by mobile messaging and instant messaging, etc.²⁵

It is probably unwise to attempt to define "unsolicited" precisely or to quantify "bulk",²⁶ as such a definition could be too rigid to withstand the evolution of the phenomenon.

Spam was quickly transformed into a vehicle for fraud and deceptive market practices (see Figure 2). As a nineteenth century police inspector in Chicago is reported to have said: "no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class". Indeed, in the open and free environment of the Internet, it was not long before the potential of this new technology was (mis)used for illegal purposes.

Figure 2: Evolution in the spam nature

Spam is not only growing in quantity, but also evolving in its nature. It went from simple text advertising to HTML messages, containing links to spam web pages, and is increasingly carrying viruses, worms and sophisticated frauds, such as phishing (see below paragraph2.2).



Source: "The Scope of the Spam Problem", E. Salem, Symanthec, online at: http://www.itu.int/osg/spu/spam/background.html

The last aspect, phishing, is probably the mostly likely to cause major concerns for operators, online companies and users, as it has the potential to undermine not only the utilization of e-mail services, but also the image of the Internet in general as a reliable and secure tool for commerce, communication and services. This could ultimately affect the right to communicate or trade.²⁷

2.1.1 Wireless spam

Spam activities are now spreading to mobile phone multi-media messaging and instant messaging services.

The use of messaging—from simple SMS to MMS to Internet e-mail—has become one of the most successful mobile applications, and the combination of mobile with Internet and IP-based technologies (such as third-generation mobile services and wireless Internet) raises a host of possibilities for innovative applications and new modes of interaction.²⁸ However, these opportunities have also been promptly spotted by spammers, who have begun to target mobile users. Considering that the number of mobile users worldwide has passed one billion,²⁹ outnumbering fixed-line subscribers and making mobile the dominant communication technology of today, it is easy to imagine the potential impact of spam on mobile devices.

As the so-called third generation of wireless networks emerges, wireless advertisement, in the form of emails delivered to cellular phones, can offer consumers time- and location-relevant information.³⁰ While this has the potential to provide attractive services to users and open the way for online mobile commerce, it is also likely to raise privacy concerns, affect efficiency and reliability of services, and diminish consumer trust.

Some mobile operators consider that mobile spam will not have the same diffusion as e-mail spam, as mobile technologies—in contrast to the Internet—were not deployed on open networks, and the costs of sending messages are usually borne by the sender.³¹ This certainly affects two of the attractions for spammers, i.e. the low cost of sending thousands of e-mails and the difficulty of tracing communications (practically guaranteeing anonymity of the sender). But two further factors must also be considered: first, in some countries, the receiving as well as the sending party pays for the message. Second, the convergence of technologies and increased interaction between the Internet and mobile technologies mean that some of the problems that hitherto only affected the Internet now may also increasingly affect mobile networks.

In Japan, where a "receiving party pays" system is used, it has been estimated that some 90 per cent of spam is sent to mobile phones, for the most part consisting of advertising for dating websites. NTT DoCoMo, one of the main mobile operators, has experienced significant problems with spam since mobile messaging was established with an open e-mail approach. The company is currently studying several solutions to help its customers, providing tools and filters to block unsolicited incoming messages, warning users about use of addresses, and even handing out free messages to compensate for unwanted messages received, in order to encourage customers to continue using the services. The issue is also being addressed by the legislator, and specific measures are foreseen for unsolicited messages sent to mobile devices. The same statement of the space of the same statement o

Problems with mobile spam are also being encountered in the United States, where—again—the receiver pays for SMS messages. The potential for such an uncontrollable expense has caused a certain reluctance among corporations and consumers to take-up wireless data services. During a recent conference on Messaging Anti-Abuse, which was held in London at the beginning of June 2004, it was reported the US operator Sprint was already blocking up to three million messages a day.³⁵ The US Federal Communications Commission (FCC) is currently soliciting public opinion about the possibility of establishing appropriate regulation to deal with wireless spam. A decision could be taken by the end of 2004.

Direct marketeers consider that advertising on mobile devices could be even more effective and successful than e-mail marketing. Aware of the dangers of mobile spam, some marketing associations are already developing codes of conduct, and hope that the fear of spam will not hamper the potential of m-marketing and m-commerce.³⁶ The Mobile Marketing Association (MMA) established privacy guidelines for its members in 2001. The guidelines are based on the premise that wireless advertising should only be sent to customers who have asked for it (following an "opt-in" approach).

It can be argued that consumers are more sensitive to mobile spam because mobile devices are more personal, with the invasion of privacy entering a more private sphere. The effect of mobile spam can therefore be seen as being even more disruptive than computer spamming. For these reasons, despite the availability of new technologies, some mobile operators have hesitated to launch services that have increased interactivity with the Internet, for fear that they might bring more spam to mobiles.

To address these concerns and to avoid being outpaced by the rapid evolution of services, legislation should be "technology-neutral" and able to withstand new means of electronic communication. Mobile operators are particularly active, some of them adopting self-regulation to try to coordinate their actions and address the problem in a timely and effective manner.

The content of mobile spam can vary, and definitions have still to be established. As mentioned above, some 80 per cent of unsolicited commercial messages, received in Japan, advertise dating websites. In the United Kingdom, a typical SMS spam message announces to the recipient that he or she has won a prize and invites them to call a Premium Rate Service number (which may cost USD 3-4 per minute). These promises are rarely fulfilled, and the numbers are often set up purely as a scam.³⁷

Messages from companies advertising promotions and prizes for games are also common in other European countries, with some being sent by mobile operators themselves. On a different note, in Italy citizens received a message from the Presidency reminding them to vote for European elections. While this kind of message cannot be deemed as "commercial", some users felt that they had been spammed nonetheless.

It is also important to realise that the gathering of mobile phone numbers is not as difficult as it may seem. Many websites offering ringtones and logo downloads are a rich source of mobile phone harvesting. Again, the principal concern here is privacy, immediately followed by loss in efficiency of messaging services, the very success of which is founded on simplicity and moderate costs—advantages which are now under threat from spam.³⁸

2.1.2 Spam over instant messaging—or "Spim"

"Spim" is to chat users what spam is to e-mail users. Spim is usually constitutes a one-line message with a link to a website. In most instances, these messages link to pornographic sites, but links to instant messaging (IM) games or software, which contain spyware, are also becoming more common. Spyware sent in this manner sends IM messages to other contacts in the user's buddy list, rapidly propagating the unwanted message and making it appear to originate from a known contact. Such "worm spam" does not, as yet, contain malicious codes or viruses, but operators are concerned that damage could be caused in the future.

Spam over IM may seem a minor problem compared to e-mail spam, but it is nonetheless a problem, particularly for corporate users. Because of the pop-up nature of IM, for instance, this kind of message can be more disruptive for users. Moreover, as spim worms propagate via IM buddy lists, spam may appear to originate from the company itself, to the detriment of the company image. AOL, one of the first targets of spim, is already trying to take counter-measures to block the spread of the phenomenon, for example by including spyware detection features in its latest version of AIM (AOL Instant Messaging).

Today, according to IMLogic figures, Spim accounts for five to eight per cent of all business IM communications, but can reach up to 17 per cent. In 2003, about 400 million spim messages were sent. It has been estimated that this number is likely to grow to 1.5 billion by the end of 2004, representing a growth rate which is triple that of traditional e-mail spam.³⁹

2.2 Spam, viruses and fraud

Spam did not remain merely an annoying marketing method for long, and quickly evolved into a vehicle for scams, misleading trade practices, offensive content and dangerous viruses. In addition to cost and wasted time, unsolicited commercial e-mail also poses security risks, including:

- Violation of privacy: Collection of e-mail addresses is often carried out without users' knowledge, and is used indiscriminately. Most spammers harvest addresses from websites by hacking into private databases, or buying e-mail lists in violation of laws on privacy and data protection. ⁴⁰ Furthermore, spam (and mobile spam in particular) constitutes a significant intrusion into the user's personal sphere.
- Identity theft: "Phishing"(see Box 1) and scams are distributed as spam, directly leading to identity theft and fraud. According to the Anti-Phishing Working Group, phishing spam increased by 52 per cent in January 2004. Also on the basis of the Working Group statistics, the response rate to these frauds is around five per cent. This phenomenon has, until now, been mainly limited to Anglophone countries, but it is only a question of time before it spreads to other countries (see Figure 2).⁴¹
- Viruses: New viruses, worms, and "malware", such as Melissa, Love Bug, and MyDoom use spam techniques to propagate after being triggered by the user.
- Combining viruses and spam: Spammers are always discovering new techniques for sending spam without being traced. One of them consists of spreading viruses and worms which install open proxies that can be used to relay spam, or that install software which transforms a computer into a "zombie", i.e. a computer owned by an unwitting user, through which spam is sent. As spam becomes more prevalent, the use of spyware is likely to increase.
- Advertising illicit/offensive content such as pornography, which is sent indiscriminately to all users, regardless of age.

As well as violating anti-spam laws--where these exist--either because of it content, or the way in which is has been sent, spam also breaches privacy laws, constitutes fraudulent behaviour, and its often offensive or disturbing content creates problems relating to the protection of minors from pornographic material.

A 2004 report by the US Federal Trade Commission has listed the top ten Internet frauds, several of which are typically perpetrated through spam messages.⁴² For example, foreign money offers (the "Nigerian letter" scam, created more than 100 years ago, has taken on a new life online)⁴³, false or deceptive business opportunities, and, more recently, ID theft (with the method known as "phishing").

Box 1: "Phishing" in the Internet sea

The word "phishing", recalls the sound of fishing, and well represents the activities of these scammers, using email lures to "fish" for passwords and financial data from the sea of Internet users. The particular spelling "Ph" is a common hacker replacement for "f", and is a nod to the original form of hacking, known as "phreaking".

Phishing is a scam attempting to trick recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. by sending messages that direct them to legitimate-looking websites masquerading as the site of a trusted financial institution or online merchant. The information is then used to access their accounts and drain money.



www.citibank.com:ac%398HAAA9UWDTY AZJWVWAAAA9pYWwgc2l6ZT00PjxTVg c2l6ZT00PjxT3Aac%398HAAA9UWDTYA ZJWVWAAAA9pYWwgc2l6ZT00PjxTVgc 2l6ZT00PjxT@211.155.234.84

Spam frauds are having a huge impact on users and online operators, who are facing new risks and costs. Recently, it was estimated that phishing attacks cost about 1.2 USD billion to banks and credit card institutes. The number of users falling in to the phishers net is also quite high: the anti-phishing working group estimate that about the 5 per cent of phishing emails are successful. In the US Gartner research revealed that 3.4 per cent of the US population have already been the victim of ID theft (see figure below).

For the moment phishing attacks have targeted US based companies, such as Citibank, Paypal or AOL, and are in English. However, these kind of scams will quickly spread to other countries (and languages): the anti-phishing working group affirmed that in 2004 a phishing attack took place on Swiss banks.

Cost	Description	Source
USD 60 billion	Cost of Identity theft in the last 5 years in US	FTC
600 hours	Individual time spent recovering from identity theft	Identity Theft Resource Center
3.4%	US Population fallen victim to identity theft	Gartner
3%	Estimated number of people reporting fraud to FTC	FTC

It has been estimated that about 90 per cent of "phished" emails have a spoofed FROM line. The suggestions given by online operators and the anti-phishing working group include, of course, the necessity to raise consumer awareness on this problem, and to provide more accurate information. Legal measures are usually already in place, as fraud is considered a crime in all countries. The problem again is the identification of phishers. For this reason the utilization of authentication standards could greatly contribute to curbing the phenomenon.

Sources: "The Scope of the Spam Problem", E. Salem, Symanthec and "The Rise of Phishing" D. Brunswick, Anti-Phishing Working Group online at http://www.itu.int/osg/spu/spam/background.html. See also Anti-phishing Working Group, at http://www.antiphishing.org/.

Fraudulent schemes—which can prove highly lucrative—are becoming more complex. In particular "phishing" is a rapidly growing phenomenon that has come to the attention of authorities, users and online operators. Phishing is used to trick recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers by sending messages that direct them to legitimate-looking websites masquerading as the sites of a trusted financial institution or online merchant. The information is then used to access and drain money from their accounts.⁴⁴

In the United States, phishing is now the fastest growing form of consumer theft. Recently-published research concluded that some 57 million consumers in the United States had received a phishing e-mail

during the last year. The most-targeted businesses have typically been the Web auction giant eBay and its PayPal payment-services division, with the financial institution Citibank serving as another popular target (see Figure 2).

2.3 The impact of spam

One of the problems surrounding the issue of spam is that there is a contradiction between the nature of the Internet, which has generally been open and free, and the desire of e-mail users to be free from unwanted commercial solicitations. Furthermore, a contradiction exists between the business interests of commercial enterprises that are looking for new avenues for marketing their products, and the interests of private individuals who do not always want to receive advertising or offers. What is at stake is the right to communicate and trade.

The shifting of the cost involved in sending spam away from the advertiser and onto the consumer and other parties is one of the major causes of the proliferation of spam. The fact that the cost of sending e-mails does not increase in proportion to the number of messages sent only encourages marketeers to send out as many copies of their e-mail as possible, with numbers that run into billions sent per day.

Internet users incur the material cost of the time spent consulting, identifying and deleting unwanted messages. From the point of view of professional and business users, spam is therefore costly in terms of productivity loss, increased need for technical support and software solutions such as filters, and the consequent impact on the reliability of e-mail as a communication tool (legitimate messages can be blocked by filters or be lost among a large number of unsolicited e-mails). As spam may contain attached files with hostile viruses, it also threatens the security of a company's internal network.

While commercial users are more worried about the reliability of communications, security and cost, private users are rather concerned about the content of these messages. With the rise of broadband, families and private users today have the possibility of an 'always-on' fast Internet connection. The development of e-commerce allows them to buy books, organize their trips online, book plane tickets and hotels. However, the new possibilities offered by this enabled environment are hampered by spam and its content. The goods or services offered for sale are often of a dubious nature. Some messages are misleading and fraudulent, such as those trying to steal a credit card number, or which install spyware on their machines, while others are offensive. As shown in Figure 2, about one message in every ten is recognized as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender. Added to this should be phishing and brand-spoofing type messages. The fact that sexually explicit material—which constitutes around 16 per cent of spam—may be sent to minors and children is also a major cause of alarm for many parents.

Figure 3: Spam content

Usually spam emails advertise anti-spam products, mortgages, or get-rich-quick schemes, but also try to sell deceptive products or to perpetrate scams and frauds. The largest part of spam emails is still in English (as they often come from the US).





Source: Brightmail statistics 2003-2004 online at http://www.brightmail.com/spamstats.html.

Apart from end-users, the other major victims are the ISPs that must process e-mails. Servers become congested when inundated with the large volume of spam messages, and large amounts of bandwidth and storage space, together with processing capacity, are consumed. Immaterial damages can include loss of reputation, and therefore of business. Furthermore, the cost of increasing bandwidth and storage capacity to deal with spam is inevitably subsequently passed on to the consumer in the form of higher access fees. Some ISPs are also predicting the end of free e-mail, or at least the creation of two-speed mail boxes: those for which it will be necessary to pay, protected by filtering and other techniques to limit spam, 45 and those that remain free of charge, which will be probably invaded by unsolicited messages, which could make them unusable.

Unsolicited messages are causing even more radical problems in both developing and least developed countries, taking up a valuable part of their already limited international Internet bandwidth. These countries often have only a few Mbit/s of connectivity, provided via satellite links, and are, therefore, particularly expensive. The consumption of part of this capacity by the bulk of unwanted emails therefore increases the cost of Internet access, reduces the quality of service (which will be even slower) and may even result in a denial of services on the networks.⁴⁶

As is clear from the above, in addition to cost, time, and wasted effort, spam is also disrupting e-commerce and other businesses to an incalculable degree, lowering user confidence and threatening network integrity and security, therefore discouraging the development and utilization of the Internet as a whole.

3 Technical solutions and legal environment: cross-border issues

3.1 Technical solutions

Technically speaking, there are three different stages in the e-mail system where measures to curb spam could be implemented: at source, where the e-mail is being sent out, at the destination, where the e-mail is received, and finally at the end-user point. At each stage, various technical measures are available (see Figure 4).⁴⁷

Technical solutions often represent the user's first line of defence against spam. Anti-spam technology is in a status of continuous flux, due to the continual adaptation by spammers attempting to circumvent it, engaging in a sort of "arms race" with operators.

Spam filtering software remains the most popular tool, and several different methods are combined to provide the best service to users. Filters, used at the ISP level or directly at the user level, can block a high percentage of spam. However there is the inconvenience of blocking also legitimate e-mail (*false positive*), diminishing the reliability of electronic communications. In addition, filters are quickly outpaced, as spammers have also become increasingly sophisticated in their attempts to evade filtering techniques, and their constant updating involves a significant extra cost for users and providers.

Rather than blocking single messages, several ISPs are using blacklists to block e-mails coming from ISPs which are considered spam sources. This system could be an efficient system as it blocks the service provider, which can then decide to stop the delivery of spam messages in order to be 'accepted' again. However, there are certain disadvantages, particularly, to the innocent customers of the blocked ISP. Several companies have sued the groups maintaining these lists for defamation or unfair business practices. Lawsuits have obtained mixed results, and on several occasions the courts have ordered the removal of the name of the plaintiff from the blacklist.⁴⁸

The purpose of filtering techniques is not to eliminate the problem at its source, but merely to contain it, creating obstacles to average spammers who do not dispose of the tools and knowledge to circumvent them. Considering the huge profits that can be generated by spam, these disincentives will not be enough to dissuade them from spamming.

Figure 4: Technical approaches to countering spam

Source

Email Server

Authentication
Payment

Destination
Email Server

•Rate limiting
•Reputation System
•Checksum

End user

Email Client

•Static Filtering
•Adaptive Filtering
•Reputation system

Source: "Curbing spam via Technical Measures: An Overview", online at http://www.itu.int/spam

Considering the limits of this approach, alternative technical solutions have started to emerge in the last few months. In particular, the current Internet protocol (SMTP), which allows any e-mail client to assert any identity in the header of the message, is one of the major causes of spam – as it makes it possible for the sender to disguise his or her identity and remain anonymous. The development of authentication systems is seen as key to solving this problem.

Spammers use a wide variety of techniques to hide their IP addresses, including the forging of e-mail addresses, spoofing, open relays and open proxies. The FTC has reported that today about 60 per cent of spam messages have some element of falsification.⁴⁹ Furthermore, the utilization of zombie drones is increasing, and some authors estimate that already about the 80 per cent of spam emanates from contaminated computers.⁵⁰

Authentication mechanisms provide a method of authenticating a sender's IP address, and can therefore block e-mails with spoofed addresses or unidentified origin.⁵¹ Several solutions have been proposed by private ISPs, such as Yahoo's Domain Keys, AOL's Sender Policy Framework, Microsoft Caller ID or the newer Sender ID.⁵² The Internet Engineering Task Force (IETF) has established a working group to develop an authentication standard to eliminate spam that uses a spoofed sender address⁵³ However, to date, all proposed methods embrace different approaches and so far there is no convergence toward a unique authentication standard.⁵⁴

Technical measures should therefore be combined with an effective legal framework. Such a combination has the potential to drive up the cost of spamming until it is too risky or no longer profitable for spammers.⁵⁵ At the same time, this is not going to be enough since spam is only a small part of the Internet's larger security problem. Some players are affirming the need to work directly on the Internet architecture, rather than simply trying to patch holes as they appear.⁵⁶

Some commentators have suggested that the solution lies in charging for sending e-mail. This solution seems difficult to implement, both for technical reasons (how to set a price for e-mail, which payment mechanism should be used, etc) and for an important social reason: users have been accustomed to sending out e-mails for free since the early days of the Internet and it would be an uphill challenge to go against this tradition, embedded as it is in the concept of the Internet as a freely accessible network. As one commentator has said, charging for e-mail would "change the whole complexion of the net".⁵⁷

In addition, when thinking about technical solutions, the needs and constraints of both developing and least developed countries should be taken into consideration. These countries, often flooded by spam messages coming from developed regions, are already struggling to extend the utilization of Internet and email, and often have neither the know-how nor the financial means to make use of updated filters or the latest antispam measures. Also, the e-stamp sort of solution would pose huge problems to users from less developed

areas, where the utilization of credit cards or other electronic means of payment is still very limited, and the spread of Internet utilization is already particularly expensive in proportion to the average GDP per capita.⁵⁸

3.2 Legislation

Spam is a "horizontal" issue, touching different aspects of telecommunications, trade, privacy and consumer protection. Accordingly, the legal framework that has been put in place in order to fight spam is complex, owing in particular to the multitude of different laws that have been enacted in recent years, and the several national authorities that are dealing with this topic. The legal definition of what constitutes illegal spam varies depending on jurisdiction, and non-spam-specific legislative measures such as legislation on privacy protection or on fair commercial practices are used to address issues arising from spam. Furthermore, legislation needs to be completed by effective enforcement measures, which should be administered by an appropriate national enforcement agency. As has been affirmed in several instances in recent months, the list of potential offences that spammers could commit is extensive, and tracking down spammers in cyberspace is more difficult than developing legal theories under which to charge them.⁵⁹

3.2.1 Spam laws

Anti-spam laws vary considerably in their approach to tackling the problem. However, unsolicited commercial e-mails are generally considered illegal when they:

- Conceal the sender's identity, for example with the falsification of the point of origin and transmission path of unsolicited e-mail advertisements;
- Use of a third party's domain name without consent;
- Provide misleading information on the subject line.

Also, for e-mail to be legitimate, many anti-spam legal instruments require:

- The prior authorization of the recipient (opt-in approach) or the existence of a prior business relationship before the sending of any commercial e-mail ("soft" opt-in approach). In some countries, where this approach is considered too severe and limiting for commercial initiative and freedom of speech, unsolicited emails, in themselves, are not considered illegal, but they must include opt-out information allowing a recipient to no longer receive commercial communications from a certain sender (opt-out approach).
- Senders to clearly indicate their true name, geographical location and e-mail address of the sender;
- A procedure for address gathering which respects the right of privacy in the processing of personal data in the electronic communication sector;⁶⁰
- In some countries, the use of a label to warn about the content of a message.

While a comprehensive analysis of world anti-spam laws is beyond the scope of this paper, a short review of some commonly used legal requirements are discussed below.

- Sender identification

The first two requirements mentioned above are included in most of the legal instruments currently in force, as one of the main problems relating to spam is the anonymity of spammers and the technical difficulty of tracing them, which in turn has an impact on the enforceability of laws.

The falsification of sender identity in the header of the message, besides rendering law enforcement more difficult, adds further costs to users, especially those whose addresses are often spoofed by spammers, "borrowing" valid addresses to create an appearance of legitimacy for their messages (an email coming from a valid address as a higher possibility to receive attention), and avoid to be inundated by bounced messages and complaints, which are directed to an innocent third party.⁶¹

Governments are now becoming more involved in the matter, as they increasingly recognize the necessity of developing and applying such standards and of ensuring that they are internationally accepted. Although it would appear that technical solutions to spam and the problems of jurisdiction and enforcement in the Internet environment are unconnected national and international regulation of technical measures adopted to limit spam may prove to be the only efficient method to control spam.⁶²

- Labelling

The use of labels for e-mails having a specific content is a requirement in several countries. Often this condition is imposed only for messages having a sexually explicit content, to warn the recipient about the content of the e-mail, and in particular to avoid spamming children, who are often the unintended recipients of adult spam. Labels for commercial messages have also been imposed in countries such as the Republic of Korea. The use of a specific tag in the subject line of an e-mail allows users to identify commercial messages more easily, to set their filters—for example by redirecting the messages to a specific folder—or to avoid their children receiving e-mail messages with pornographic content. The problem, once again, is that the rule is difficult to enforce in respect of anonymous spammers.

A second possible problem arises even in the case of legitimate marketeers who operate within the law. These labels are decided at the national level and vary from country to country, leaving the way open to messages originating from another country that does not use the same labelling system, causing an inevitable lack of uniformity.

For example, in April 2004 the FTC announced that spam containing sexually-oriented material must include the warning "Sexually explicit" in the subject line.⁶³ About one year previously, in June 2003, Korea implemented similar rules establishing that adult-oriented content must be stipulated with the subject field "Adult advertisement".⁶⁴ In this case it is easy to see how the creation of a sort of international "Internet standard"⁶⁵ might be needed, as initiatives against spam will not be effective if every nation implements different approaches, based on different criteria and different strings in the e-mail subject field.

- Opt-in versus opt-out

Much debate has surrounded the adoption of the opt-in approach for spam messages in Europe. Opt-in was considered as potentially threatening to the development of e-commerce and the Internet, and generally contradictory to overall EU e-strategy. What the EU framework tries to achieve however, is not to outlaw direct marketing altogether, but simply to establish a fair and clear environment for legitimate marketing that is permission-based, while also reducing unwanted spam.

The opt-in approach has been adopted mainly in European countries, in line with EU Directive 2002/58, which started implementation in 2003. This Directive is based on an earlier one on data protection in the electronic environment (EU Dir 95/46/EC).⁶⁶In the Asia-Pacific region, to date, only Australia has adopted a similar opt-in approach. This trend can be better understood when one considers that it is perhaps more in line with the traditional European values of privacy, to which the EU Directive refers.

Directive 95/46/EC—implemented by most European countries in 1998—was conceived to enable individuals to control the dissemination of their personal information, and applies to personal data wholly or partially processed by automatic systems. In particular, the data must be "collected fairly" (excluding harvesting techniques or violation of private databases) and used for "specified, explicit and legitimate purposes" and not "in a manner inconsistent with those purposes" (art. 6b). This rule is then recalled by Article 2 of Directive 2002/58, which foresees an exception to its opt-in approach, allowing the sending of unsolicited commercial messages to users with whom the sender has a pre-existing business relationship. This exception, however, is applicable only for the advertisement of "similar" products and services, and the addresses must be used by the same person who legally collected the original data. (soft opt-in).

A further exception to the opt-in approach is foreseen where the recipient is not a physical person but a legal entity. In this case, member countries have the possibility of choosing between the opt-in and opt-out approaches, provided that they respect the legitimate interest of subscribers with regard to unsolicited communications. This exception is, however, subject to criticism, as business-to-business spam could have the same nature as spam sent to private users.⁶⁷

The second approach, opt-out, considers direct marketing—and therefore unsolicited commercial communication as a legitimate activity, unless certain conditions are not respected. Opt-out has been preferred in the United States, which adopted it at the federal level with the CAN-SPAM act, but also in Asian countries, such as Japan and the Republic of Korea. With this system, marketing companies are allowed to send messages to users without the need for prior authorization or relation, provided that explicit opt-out language is included in every message.

This approach has been criticised as it can actually contribute to legitimate spam, condemning only unsolicited e-mails that have an illegitimate content, while letting bulk e-mailing proliferate.⁶⁸ Most users, however, already have strong preconceptions regarding spam, and have been widely advised not to open or reply to any spam messages, to avoid confirming that the e-mail address is active.

The harmonization of legislative approaches to spam between different jurisdictions from which an e-mail user is likely to receive spam would be crucial in order to properly tackle the problem.⁶⁹ Notwithstanding the long debate surrounding these two different approaches, many experts consider that it would be more important to develop effective enforcement measures that empower enforcement agencies to act against spam, and to promote cooperation among the different jurisdictions from which an e-mail user is likely to receive spam.

As mentioned above, the majority of spam received by users is not sent by legitimate marketeers, but by individuals concealing their identity or exploiting third-party relays, who are therefore not concerned by any legal requirements to request prior consent.

3.2.2 Non-specific spam laws

Spammers usually violate more than one legal provision against spam, in addition to other related laws—for example—to privacy and data protection, contract law, private property, image and trademarks.⁷⁰ Depending on the content of the e-mail—their activity can also constitute fraudulent behaviour, violate laws on fair competition, and so on.

Tired of bearing the increased processing costs of bandwidth and storage, the wrath of customers and loss of reputation, ISPs have been among the first to have decided to initiate litigation against spammers. As most ISPs have contractual agreements with their clients, service providers have, for example, sued spammers for breach of contract. One such case is that of Hotmail Corp. versus Van Money Pie Inc. In this case, the court found that the defendant had breached the Hotmail subscriber's service agreement, which explicitly prohibits the sending of unsolicited bulk e-mail. Other ISPs however, have less clear policies, referring in general to respect of Netiquette or of codes of conduct.⁷¹

In another case, that of CompuServe versus Cyberpromotions, the ISP claimed that sending e-mails through its computer equipment could be considered a trespass of personal property. In that case, the judge retained that violation of personal property can be committed by "intentionally using or intentionally bringing about a physical contact with the chattel in possession of another". The application of the trespass doctrine can however prove ineffective, as many spammers are using different accounts or network providers for each unsolicited advertisement sent, and tracking down a spammer is becoming more complex—Cyberpromotions was an identifiable company, while most of today's spammers remain anonymous. The company of the company o

Other than the trespass claim, false designation of origin has also been used. In the 'AOL versus IMS' case, it was considered that the defendant falsely designated the origin of his e-mail as coming from AOL and therefore deceived recipients and had caused damage. Trademark violation has also been used in cases of e-mail header forging. AOL successfully claimed that the unauthorized use of the AOL trademark within the e-mail header constituted trademark infringement, reducing the distinctive quality of a well-known service mark through the negative association with the defendant's use.⁷⁴

Claims based on violation of privacy and data protection are more common in European countries. As mentioned above, protection mechanisms for the treatment of personal data in the electronic environment were already in place in 1995, and are based on a "right to privacy", which is considered fundamental in Europe. An e-mail address is unique to an individual user and therefore is considered as personal data. The collection of e-mail addresses through harvesting techniques, or their utilization for reasons other than the purposes for which they were initially collected, is considered a violation of the directive (and of the national laws implementing it) and is therefore illegitimate.⁷⁵ The same is applicable in Argentina, where there is no specific anti-spam legislation as yet. The data protection law has recently been at the base of a claim against a company that is using illegally gathered e-mail addresses, which the court considered as "personal data which deserve protection".⁷⁶

Other legal reasons for pursuing spammers can be found in the content of the unsolicited message. As mentioned above, spam can be the vehicle for deceptive market practices, misleading advertising or frauds⁷⁷ and may therefore be covered by the relevant national laws. Usually, penalties are stiffer for more serious

cases, and include criminal sanctions. 78 The Federal Trade Commission (FTC) has often used deceptive practice legislation to bring action against spamming organizations, on the basis of the deceptive content of the message. 79

The above examples give some idea of the multiplicity of channels that can be used to legally sue spammers, and of the multitude of authorities involved, including data protection authorities, telecommunication regulatory agencies and consumer protection authorities. This brings us to the topic of enforcement.

3.3 Enforcement

Together with jurisdictional barriers, practical issues relating to enforcement are the most significant barriers to developing legal responses to spam. E-mail is generally unaffected by national boundaries because of the borderless nature of the Internet. Many e-mail addresses provide no indication of the addressee's (e.g. .com, .org) physical location and an e-mail address that includes a geographic identifier (such as .fr, .us, .it) can be used from anywhere in the world. Even if a State is able to exercise long-arm jurisdiction over a foreign defendant, it may be difficult to locate and subsequently enforce a judgment on someone who is in another State or country

In addition, enforcement of the provisions regarding unsolicited commercial communications is not performed by the same authority in all countries. In most cases, it is the Data Protection Authority (DPA) in a particular country that deals with spam as a breach of privacy and is therefore in charge of taking decisions on the application of the law, and on enforcing the rules in the first place. This is the case, for example, of most European countries, such as Italy and France, but also of Argentina and New Zealand. The National Regulatory Authority (NRA) for telecommunication may also be involved in the spam battle, as is the case of the Australian Communication Authority, which is very active in the field of spam, but also in Ireland and Singapore. In some cases it is the consumer protection authority (CPA) which takes the lead in the enforcement of anti-spam laws, as is the case for the FTC in the United States.

As is often the case with Internet matters, most countries do not have a single "Internet authority" dealing with spam, creating some confusion at the implementation level, but also for the eventual development of international cooperation. In the United States, while the FTC is in overall charge of issues relating to spam, as a subject relating to consumer protection, wireless spam is under the responsibility of the telecommunication regulator, the FCC. In the United Kingdom, the Information Commissioner is in charge of spam matters, although other governmental bodies are also involved, such as the UK office of Fair Trading and Her Majesty's Secretary of State for Trade and Industry in the UK, which are also signatories of the recent MoU on Mutual Enforcement Assistance in Commercial Email signed among enforcement agencies from the United Kingdom, United States and Australia.⁸⁰

While more and more countries are currently developing anti-spam legislation in an effort to limit the phenomenon, the spam cases brought to court are still very limited in number. This is due in particular to the fact that spammers are using increasingly sophisticated techniques to hide their identity and the origin of their e-mail, so that prosecution becomes a long, time-consuming and expensive task. ⁸¹ One commentator, in a recent paper, considers that to draft an effective anti-spam law it is not sufficient to include all the elements that make a message "spam", but also action-oriented rules and empowering enforcement mechanisms. ⁸²

The difficulty of identifying spammers, and enforcing laws against them, adds to the reasons why spamming is so easy and considered a low-risk profitable business. Not only do spammers not have to bear high operational costs, but also the barriers to law enforcement and anonymity render the threat of punishment an ineffective means to ensure compliance with anti-spam laws.

Spamhaus claims that 80 per cent or so of all spam e-mails sent globally are sent by a handful of spammers, and that stopping those individuals would dramatically reduce the problem. This view has been taken on board by some of the largest ISPs in the world, Yahoo!, EarthLink, AOL, and Microsoft, which in 2004 decided to join forces to track down and sue the biggest spammers in the United States. The court trials can be particularly expensive also for spammers, creating additional costs and directly cutting their revenues. If the risks and costs of spamming were raised, one of the main drivers of spam would be eliminated.⁸³

Even when good and effective legislation is implemented in one country, it cannot stop unsolicited e-mail coming from other countries. In the United Kingdom, users consulting the "Information Commissioner" (authority for data protection) website can find a page where the Government explains what it is doing to

eliminate spam, but after a short overview of the law requirements (opt-in), it is clearly stated that this law is applicable only to messages coming from United Kingdom, and that as most of the spam received in the country is from the United States, there is not much that can be done, legally speaking.⁸⁴

Conscious of the limits of the national approach, governments are today trying to create a framework for international cooperation on technical and legal issues to curb the proliferation of spam.

4 International initiatives in the field of spam

The jurisdictional problems created by the proliferation of trans-border unsolicited commercial communications represent what may prove to be an insurmountable hurdle. As spam touches on so many aspects of the law – such as commerce, advertising, criminal law, freedom of speech, and intellectual property – the differences associated with the laws of the jurisdictions of the world may prove greater than their similarities.

While it is important to act at the local level—by creating, for example, an appropriate legal anti-spam framework, building awareness, educating consumers and establishing dialogue and partnership with the private sector—any anti-spam measure should be considered at the international level.

International cooperation has two objectives in the case of spam: to promote the adoption of effective legislation and common standards in countries that do not yet have them, and to encourage countries to cooperate with others to ensure effective enforcement of applicable rules. While several initiatives have been undertaken in the past few years to fight spam, a multilateral coordinated international framework is still lacking.

• Multilateral cooperation: The Australia, United Kingdom, United States Memorandum of Understanding (MoU) on mutual enforcement assistance in commercial e-mail matters

On 2 July 2004, a Memorandum of Understanding (MoU) was concluded between the US Federal Trade Commission, the UK Office of Fair Trading, the UK Information Commissioner, Her Majesty's Secretary of State for Trade and Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority. The MoU provides for the agencies to share information, cooperate in detecting and investigating spam violations, cooperate in tracking spammers, exchange evidence, facilitate law enforcement against spam violators, and coordinate enforcement against cross-border spam violations.

This MoU constitutes an important step to help law enforcers on three continents leverage resources to combat illegal spam, and provides a framework for cooperation in fighting cross-border spam affecting all three countries.⁸⁵ Although it does not include types of spam other than e-mail spam, this MoU should constitute a good start towards more extensive cooperation on the subject.

The agreement is in line with the policy towards improved international cooperation in the field of spam promoted by Australia in recent months. The role of collaboration between agencies in different countries, and exchange of information is stressed in this instrument, which, being concluded by players already very active in the field of the anti-spam battle, could go further, establishing cooperation between national agencies in enforcement actions. This is part of two-layered international approach. A first layer focusing onto the sharing of information about workable anti-spam legislation and complementary measures, the second one more oriented towards cooperation and joint enforcement.⁸⁶

To follow up to this Memorandum, a meeting is planned to take place in London in October, gathering all national agencies members of the ICPEN. This could be the first step towards an enlargement of the cooperation on enforcement for these countries already having implemented an anti-spam legislation.

• Bilateral cooperation: The Australia-Republic of Korea Memorandum of Understanding (MoU) concerning the regulation of spam

In October 2003, an MoU on the regulation of spam was signed between the Korea Information Security Agency (KISA) and the Australian Communication Authority and National Office for Information and Economy of Australia.

The agreement was concluded to encourage cooperation between the agencies in minimizing spam that originates and is sent to end-users in Australia and Korea. Within the terms of the MoU, the agencies of the two countries will work closely together, exchange information relating to spam and will try to develop cooperative mechanisms to combat the rapidly growing spam problem. This collaboration could be extended in the future to include joint enforcement actions.

With this MoU, Australia and Korea are leading the international effort to address spam, also encouraging other national communications regulators to work to develop a multilateral MoU in this field. A standard MoU could be used for a multilateral approach to agreements, simplifying the establishment of international cooperation principles for locating and dealing with spammers.⁸⁷

• European Union

The European Union, by Directive 2002/58, was one of the first players to try to create harmonized international regulation dealing with spam at the European level. The Directive is, however, considered just a small step in the general EU e-strategy, and only a first step in the fight against spam.

The implementation of the Directive in the different EU countries has been a lengthy process. The differences in implementation and the confusion that is still present at the national level regarding identification of the responsible authority, adds even more difficulties.

In its communication on unsolicited commercial communications,⁸⁸ the European Commission recognized effective law enforcement as one of the most important elements in the fight against spam, and still one of its weakest points. The Commission then decided to continue its investigations in order to understand which would be the best mechanisms to put in place to ensure efficient enforcement of anti-spam legislation. Furthermore, it is encouraging improved collaboration among members and has proposed the creation of national liaison offices under the national regulators, in order to establish a network to support cooperation.

The Commission realized that actual enforcement could be particularly difficult in relation to third countries, notwithstanding the opt-in rule for all unsolicited commercial communications which are sent from *and* received on networks in the Union. Nevertheless, the Commission still deemed it essential, considering that most of the spam received in European countries comes from outside EU borders.

The lack of appropriate international cooperation mechanisms is evident therefore, and is also seen by European authorities as one of the major obstacles to enforcement. For this reason, the EU is promoting the development of international initiatives in this field, and is inviting its members to engage in bilateral cooperation with third countries, not only for the promotion of effective legislation, but also for cooperation on enforcement, including police and judicial cooperation, where appropriate.⁸⁹

The fight against spam has a place in the larger EU e-strategy framework, as one of the elements which could hamper the diffusion of broadband in the European territories. In a recently held roundtable comprising European telecommunication ministries and industry CEOs from the telecommunication media and technology sector, a list of six strategic actions to stimulate the growth of broadband was presented by the industry to governments. The first point on this list indicated the need for "timely implementation of effective anti-spam, privacy and security regulatory frameworks". Two specific initiatives were suggested: one regarding effective enforcement mechanisms, the other stressing the necessity to develop a joint EU-US action plan to address spam originating in both territories. 91

• International Telecommunication Union (ITU)

During the 2003 Global Symposium for Regulators a recommendation was made that the ITU launch a discussion on frameworks for international cooperation on countering spam. Following this recommendation a virtual conference on regulatory cooperation on spam was held at the end of March. ITU decided to hold a WSIS Thematic Meeting on Countering Spam, to gather all interested stakeholders and discuss possible international cooperative solutions to this scourge. IThe meeting gathered representatives from about 60 governments, and allowed, for the first time, participants from less developed economies to express their concerns and their needs in this field. Among the several contributions made to the meeting, a special note should be made of the intervention of a group of developing countries, who affirmed the importance of raising awareness on the problems they are encountering with spam and the need to have *fora* in which they could exchange information and experiences.

Developing countries called for more support from developed countries and the international community in facing the problem of spam in particular, and Internet security in general, recognizing that, while legislation in itself is not the solution, it could indeed help in fighting this phenomenon. Their suggestion for the creation of an effective framework for international cooperation and coordination--with the active participation of developing countries, was warmly supported.

Following the conclusion of the meeting, ITU is continuing its work on countering spam, elaborating a database gathering laws, information and contact details of enforcement authorities dealing with spam worldwide,⁹⁴ cooperating with other international organizations in areas of common interest,⁹⁵ and promoting the creation of a suitable framework for international cooperation, which could lead to the adoption of a global agreement on the subject.⁹⁶

• *Organisation for Economic Co-operation and Development (OECD)*

The Organisation for Economic Co-operation and Development (OECD) has recently taken action on the issue of spam, organizing a workshop on the subject at the beginning of 2004. This workshop was organized in collaboration with the European Commission, and represents just the first step of a longer process aiming at fostering international cooperation in the fight against spam.⁹⁷

The OECD is currently continuing its work focusing on five main elements: effective anti-spam legislation, international cooperation and enforcement, self-regulation by industry, innovative technical solutions and increasing awareness and education. In the coming months, the organization is willing to build on the achievements of the first meeting and begin to develop an "OECD Anti-spam Toolkit", which could help countries in dealing with the problem in a more organized and cooperative manner. To help with the elaboration of this Toolkit and to further cooperation among different players, in July 2004 OECD Members set up a Task Force on spam.

Asia Pacific Economic Cooperation (APEC)

In the framework of its activities relating to electronic commerce, the APEC Electronic Commerce Steering Group recently agreed to undertake specific activities on spam as part of its 2004 work agenda. 98 This will include the development and of a survey on the laws of APEC economies, and spam-related self-regulatory and educational efforts undertaken by economies.

The group aims in a first instance to identify damage caused by spamming practices, and to promote the exchange of information on the cost of spam to businesses and users. Furthermore, the group will try to identify areas where domestic policies and laws could assist in preventing and respond to the damage caused by spam, and to encourage the development of cross-border cooperation among members, further implementing the APEC Consumer Protection Guidelines. In addition, during the last APEC workshop held in Santiago, Chile, the necessity to undertake cooperative activities with other organizations addressing the problem of spam was underlined.⁹⁹

• Operation "Secure Your Server"

The United States recently recognized the importance of international cooperation in the anti-spam battle—cooperation that should involve not only government or private stakeholders, but "everyone with an Internet connection". Accordingly, the US Federal Trade Commission launched an initiative at the beginning of 2004, in order to close off indirect sources of spam such as the so-called "open relays" and "open proxies", which can be used by spammers to pass unsolicited commercial e-mail through the system of an unwitting user, thereby hiding the real origin of the message.

The Commission is working to identify owners of these potentially open servers and proxies, to warn them about the risks they are incurring, and therefore urging them to protect their system from misuse. To do so in a more effective way, the Commission is seeking the cooperation of authorities in foreign countries. Currently, agencies from about 28 countries are participating in the US-led initiative. 101

■ International Consumer Protection and Enforcement Network (ICPEN)

The International Consumer Protection and Enforcement Network (ICPEN)¹⁰² is a network of governmental authorities involved in the enforcement of fair trade practice laws and other consumer protection activities. Membership in the Network includes organizations from 29 countries, most of which are members of the Organisation for Economic Co-operation and Development (OECD). The mandate of the Network is to share

information about cross-border commercial activities that may affect consumer interests, and to encourage international cooperation among law enforcement agencies.

In 2001, the ICPEN announced an Internet-based project to gather and share cross-border e-commerce complaints. National agencies from 17 countries are currently participating in this initiative, which provides consumers with an online form through which they can lodge complaints with a Consumer Sentinel, a database maintained by the US FTC. The information will be accessible to certified government law enforcement and regulatory agencies in ICPEN-member countries, and may be used to investigate suspect companies and individuals, uncover new scams, and spot trends in fraud. Following the ICPEN meetings held in 2004, the UK's Office of Fair Trading (OFT) and the US Federal Trade Commission (FTC) are organizing a Spam Enforcement workshop, which will take place in London on October 11th, 2004. This meeting will gather enforcement authorities from about 30 countries with the aim of sharing experiences and techniques of enforcing anti-spam laws, and to discuss how to enhance working-level collaboration among regulators in different countries in the fight against spam.

It is interesting to note that although all of these initiatives and projects deal with the anti-spam battle, they are implemented by different organizations, often dealing with different aspects of the problem. Looking at the agencies participating in the projects reveals that, for any given country, there may be as many as three or four different entities involved in different aspects of combating spam. Also striking is the fact that only a limited number of countries have so far become active in setting up initiatives, which usually exclude developing regions such as Africa.¹⁰⁴

5 Conclusions: Act locally, think globally

This report has shown in brief how the many approaches currently planned to fight spam will need to be coordinated, and their impact extended through international cooperation and collaboration between private and public entities.

The information society is for all, and all stakeholders have a role to play in it, and this also applies to the problem of spam. This means that each and every government, operator, company and user has a part to play.

5.1 The role of users

Internet users, whether at the business or individual user level, need to recognize that the Internet is not a simple commodity, but a tool which is increasingly becoming part of our lives. Just as individuals protect their houses from undesired visitors, they should learn to protect their computers from intrusion and unsolicited content.

In the short term, awareness-raising and education will have a fundamental role to play. User groups may work together to develop and implement best practices, share information and learn about secure practices that could limit the damage caused by spam. If the number of spam e-mails opened by unaware users is reduced, it is likely to have an impact on spam.

As the Internet has been developed by technologist users, they also have an important role in the long-term evolution of the Internet architecture, and should participate in the debate at national and international levels, to put forward their views and influence the creation of new solutions to combat the problem of spam.

5.2 The role of industry

Although market solutions have been unable to fully address the problem of spam to date, private sector has a fundamental role to play.

In the short term, private sector is fundamental for the development and application of technological solutions which can help alleviate the spam problem by imposing costs and other disincentives on spammers, and filtering the bulk of spam before it reaches users' inboxes. In this sense, the use of filters, blacklists, ISPs cooperation in legal pursuits, and the establishment of codes of conduct, are fundamental.

Several companies are already working for the elaboration of possible long-term solutions, creating consortia to exchange information and experience to develop a coordinated response to counter spam and set up

common standards for sender authentication. In this area, industry is also asking for the support of governments, which are responsible for providing an appropriate legislative framework.

5.3 The role of governments

With regard to consumers, government has a duty to improve users' education, promote the diffusion of information on secure use of the Internet and e-mails, and raise awareness of the dangers connected to the increased interaction between telecommunication devices and Internet appliances, which leave room for even greater possibility of misuse. Several governments have web pages dedicated to Internet fraud, viruses and spam. This information should also be made available through the mass media, and not only in the specialized press.

• Governments have the primary responsibility for setting up an appropriate legislative environment for cyberspace, in particular regarding unsolicited commercial communications.

Legislation should be complemented by effective application and enforcement mechanisms, to provide prosecutors with the necessary instruments to operate. The problem which has been often remarked upon in the prosecution of spammers, is that notwithstanding the multitude of different laws which can be applied, enforcement is still complex and expensive, so that judicial action against spammers can often be afforded only by larger companies which invest substantial resources in investigations. Indeed, deeper involvement and action by governments is required at this level, to increase cooperation among the national authorities responsible for administering laws that can be applied to spam, and to enforce those laws.

This kind of legislation, however, has its limits. Whichever method is used, anti-spam laws aim at punishing illegal conduct *ex-post*, and may work as a deterrent for future violations. Nevertheless, as happens with some "first line" technical solutions—such as filtering—they only intervene in a situation after the fact. Filters avoid spam cluttering up users' inboxes, decreasing the efficacy of the message; laws punish the individual infringing the rules, increasing the risk and cost related to spamming. In both cases, disincentives, such as additional costs or reduced profits, are imposed on spammers. This will help in reducing the problem, but it is unlikely to eradicate it.

• Depending on the necessity of intervention, government legislation could also be effectuated at a higher level, regulating the structure rather than the individual.

For example, it has been recognized in recent studies that, because of the simplicity of the current Internet Protocol, one of the main hurdles in the fight against spam is the possibility for senders to remain anonymous. For this reason, the development of authentication mechanisms is considered a possible solution.

While it is usually the market which influences the creation and diffusion of technical norms, in the case of authentication standards or secure Internet protocols, the market approach has not been successful to date. This is because a simpler—and less expensive—solution has been used. Recently, private companies have begun developing authentication methods. There is still not, however, a common accepted standard, and it is perhaps time for governments, in collaboration with private sector, to get involved.

The role of governments can be fundamental in encouraging the development of standards, mandating their adoption at the national level, and fostering further international cooperation and agreement for their global utilization.

While each government should act against spammers operating from within their jurisdiction, in the borderless cyberspace exchange of information, international harmonization of legislation and enforcement are crucial, and governments can actively support the trend towards multilateral and bilateral international cooperation. Australia and Korea are already providing a good example of basic cooperation in the field of spam, and several international and regional organizations are moving towards a coordinated approach to the problem. Once again, the real issue is not only to have a formal agreement, but the political will to take action and tackle this problem.

5.4 A final word

It is widely recognized that spam is a complex problem which is heavily affecting society, and it has been convincingly argued by many commentators that any single solution, however targeted and efficient, will not be enough to solve it. Trans-border unsolicited e-mail cannot be dealt with using traditional legal solutions. Moreover, self-regulatory approaches have a number of shortcomings, and technical solutions to date are only partially successful. As outlined above, a coordinated legal and technical approach, harmonized at the international level, would seem to constitute a particularly promising approach.

Although at this stage it is beyond the realms of possibility that spam will not exist anymore, if all players were to seize the opportunity to be *proactive*, rather than simply *reactive*, unsolicited commercial e-mail could be effectively tackled. Spam could then probably continue to exist in cyberspace, much as unsolicited marketing calls and postal advertising exist in the real world, but would be a mere annoyance, rather than a threat to the future of our global information society.

¹ MessageLabs statistics, see Figure 1.

² See the World Summit on the Information Society (WSIS) website at: Hhttp://www.itu.int/wsisH.

³ See: Hhttp://www.itu.int/wsis/documents/doc multi.asp?lang=en&id=1161|1160H.

⁴ See below, paragraph on International cooperation.

⁵ "Spam is still growing--and costing", ZdNet, 14 June 2004, online at Hhttp://zdnet.com.com/2102-1105_2-5233017.html?tag=printthisH

⁶ Nucleus Research "Spam: The Serial ROI Killer". Online at Hhttp://www.nucleusresearch.com/H

⁷ A research prepared by Gartner at the beginning of 2004 reveals that email frauds (in particular phishing) cost \$1.2 billion in damage to U.S. Banks and credit card issuers in 2003.

⁸ See: Hhttp://www.spamhaus.orgH.

⁹ Recent studies have indicated that a response rate as low as 1 per 100,000 e-mails sent allows spammers to recover their costs. See the paper "curbing spam via technical measures: an overview", available online at Hwww.itu.int/spamH.

¹⁰ Simple Mail Transfer Protocol (SMTP) is a HprotocolH for sending He-mailH messages between HserveHrs. A definition of SMTP is available online at: Hhttp://www.webopedia.com/TERM/S/SMTP.htmlH.

¹¹ Interview with Steve Lindberg, Spamhaus, online at H<u>www.tsr.ch</u>H; and FTC Spam Workshop, 30 April- 2 May 2003, online at H<u>http://www.ftc.gov/bcp/workshops/spam/</u>H.

The London Internet Exchange (Linx), the UK's most influential ISP organisation, has agreed tough new antispam guidelines. See "ISPs agree anti-spam code", August 2004, online at:
Hhttp://www.computerweekly.com/articles/article.asp?liArticleID=132775&liArticleTypeID=1&liCategoryID=2&liCategoryID=2&liCategoryID=2&liCategoryID=2&liCategoryID=1&sSearch=&nPage=1
H. See also infra paragraph 3 on legislation and enforcement.

[&]quot;Spam: Report of an enquiry of the All Party Internet Group (APIG)", October 2003, Hhttp://www.apig.org.uk/H; M. Geist, "Untouchable? A Canadian perspective on the anti-spam battle", May 2004, online at: Hhttp://www.itu.int/spamH.

¹⁴ The Spamhaus Block List (SBL) is a real-time database of IP addresses of verified spam sources (including spammers, spam gangs and spam support services), maintained by the Spamhaus Project team: Hhttp://www.spamhaus.org/H.

- ¹⁸ See United States "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or "CAN-SPAM Act of 2003". Online at: Hhttp://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf
- ¹⁹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), online at: Hhttp://europa.eu.int/eurlex/pri/en/oj/dat/2002/1 201/1 20120020731en00370047.pdfH.
- ²⁰ For more information about anti-spam legislation in different countries, see: Hhttp://www.itu.int/osg/spu/spam/law.htmlH.
- ²¹ "Tech firms tackle spam", CNET News.com, 14 March 2003, online at Hhttp://www.zdnet.com.com/2100-1105-992759.htmlH. Regarding cooperation between private companies, see, among the others the recent The Anti-Spam Technical Alliance (ASTA). "Anti-Spam Technical Alliance Technology and Policy Proposal", 22 June 2004, online at Hhttp://download.microsoft.com/download/2/3/7/23779c05-d409-46ce-b9d6-c24908789d8b/ASTA%20Statement%20of%20Intent.pdfH.
- ²² See M. Geist, "Untouchable? A Canadian perspective on the anti-spam battle", May 2004, Hhttp://www.michaelgeist.ca/geistspam.pdfH.
- ²³ APIG Report, supra note 13.
- ²⁴ Commission Nationale de L'Informatique et des Libertés (CNIL), Hhttp://www.cnil.fr/H. However the definition may be different for countries adopting the opt-out approach (see infra paragraph 3.2)
- Directive 2002/58/EC Of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Online at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/1_201/1_20120020731en00370047.pdf
- ²⁶ However the US CAN-SPAM Act (Sect. 4) talks about "multiple" commercial electronic mail messages, meaning "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period".
- ²⁷ See paragraph 2.2 on spam viruses and fraud.
- ²⁸ ITU Workshop "Shaping the future mobile information society", online at Hhttp://www.itu.int/osg/spu/ni/futuremobile/index.htmlH.
- ²⁹ Data at the end of 2002. ITU Internet Report "Birth of Broadband", Statistical Annex, ITU, 2003.
- 30 See E. Cramer "The Future of Wireless Spam", Duke Law and Technology Review, October 2002. Location-based marketers could direct mobile messages to the recipient, wherever he or she is, with a precise content based on location and personal characteristics.
- ³¹ The billing option "calling party pays" is typically used in mobile networks whereby the person making the call (or in this case sending the message) is charged the full cost, in contrast to billing also the recipient of the call (Receiving party pays, see note 29).
- ³² Receiving party pays (RPP) is a billing option whereby the person receiving a call is charged in addition to the person initiating the call. For example, Japanese users are billed on the basis of a fee for every packet of information they transmit or receive.
- ³³ ITU G-REX Virtual Conference on spam, 30 March 2003, online at Hhttp://www.itu.int/ITU-D/treg/Events/Seminars/Virtual-events/Spam/index.htmlH.

See J. Magee, "The law regulating unsolicited commercial e-mail: an international perspective", Santa Clara Computer and High Technology Law Journal, May 2003.. Several companies objected to being included in these blacklists, and brought to court their case against the organization that maintained the list. The results are mixed, with cases in which the court ordered removal of a company from the list.

¹⁶ Direct Marketing Association at: http://www.the-dma.org.

¹⁷ In the US CAN-SPAM Act (see note 18) the congress recognizes that "there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis".

- ³⁹ "Brightmail partners to fight instant spam", CNET News, 8 June 2004, online at Hhttp://news.com.com/2100-1032 3-5228678.htmlH.
- ⁴⁰ In June 2004 an AOL employee was arrested after having sold some 90 million e-mail addresses of AOL customers. See CNN news, 23 June 2004, online at: Hhttp://money.cnn.com/2004/06/23/technology/aol spam/?cnn=yesH.
- ⁴¹ Anti-phishing Working Group at: Hhttp://www.antiphishing.org/H.
- ⁴² Trends in fraud and identity theft, Federal Trade Commission, 2004.
- ⁴³ Internet Fraud Complaint Centre, Nigerian Letter Scam, online at: Hhttp://www1.ifccfbi.gov/strategy/fraudtips.asp#Nigerian%20Letter%20ScamH.
- ⁴⁴ Anti-phishing Working Group at: Hhttp://www.antiphishing.org/H.
- ⁴⁵ For example MSN is now offering MSN Hotmail Plus, a subscription version of the Web-based e-mail system which, for 19.95 USD/year provide 2Gb storage space and anti-spam filters which block both incoming and outgoing unsolicited bulk e-mail that carry viruses. See "MSN Announces Comprehensive Worldwide Upgrade to MSN Hotmail" online at Hhttp://www.microsoft.com/presspass/press/2004/jun04/06-24HotmailUpgrade2004PR.aspH
- ⁴⁶ See "Developing countries and spam" contribution to the ITU WSIS thematic meeting on countering spam, online at: http://www.itu.int/osg/spu/spam/contributions/Developing%20countries_contribution.pdf.
- ⁴⁷ For an overview of the current technical anti-spam solution, see Ho Khee Yoke and Lawrence Tan "Curbing Spam via Technical Measures: An Overview", paper presented at the ITU WSIS meeting on countering spam, June 2004. Online at: Hhttp://www.itu/int/spamH; D. Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail", University of S. Francisco L. Rev. (2001), p. 347.
- ⁴⁸ M. Geist, "Untouchable? A Canadian perspective on the anti-spam battle", May 2004, p. 11. Online at: Hhttp://www.itu.int/spamH.
- ⁴⁹ See FTC National Do Not Email Registry A Report to Congress, Hhttp://www.ftc.gov/reports/dneregistry/report.pdfH.
- ⁵⁰ Normal home computers can be transformed into "zombie drones" by malicious viruses or worms sent by e-mail. Those infections turn the affected computer into an open or compromised proxy, through which spam is sent out. The problem in this case is that also authentication systems could fail. See FTC "Do not e-mail registry: report to congress", p. 8-10; CNN "Your computer could be a 'spam zombie'", 18 February 2004, online at: Hhttp://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/H and The Register "Zombie PCs spew out 80% of spam", online at Hhttp://www.theregister.co.uk/2004/06/04/trojan spam study/H. The problem is felt also in European countries: at the end of June an article in one of the largest Italian newspapers (Corriere della Sera) warned users about viruses and worms infecting their PCs, transforming them into unwitting spammers.
- ⁵¹ But, for example, would not help in the case of computers infected by worms unwittingly sending out spam.
- ⁵² Sender ID is the result of Microsoft's Caller ID for E-Mail proposal, Meng Wong's Sender Policy Framework (SPF), and a third specification called the Submitter Optimization. However its adoption is already encountering many problems. See Hhttp://slashdot.org/article.pl?sid=04/09/07/231241H.

³⁴ The law (No. 26 of 2002) obligates senders of unsolicited e-mail to display the sender's name and contact information and to include at the beginning of the subject line that the e-mail is an advertisement. Also, cellular users have to be provided with an opt-out option. Violations can be reported to the MPHPT, which subsequently initiates procedures against the sender of the unsolicited message. A non-official translation of the Japanese law is available at: Hhttp://www.itu.int/osg/spu/spam/law.htmlH. See also "Spam clarity and confusion", 15 June 2004, online at: Hhttp://www.160characters.org/news.php?action=view&nid=1153H.

³⁵ Messaging Anti-Abuse Conference, 2004, London, at: Hhttp://www.openwave.com/us/events/anti-abuse_londonH.

³⁶ See Mobile Marketing Association (MMA), page on spam and privacy available at: Hhttp://www.mmaglobal.com/conduct/index.htmlH.

³⁷ See ITU WSIS meeting on countering spam, R. Borthwick presentation "Vodafone Group policy on bulk unsolicited communications", online at: http://www.itu.int/osg/spu/spam/background.htmlH.

³⁸ Messaging Anti-Abuse Conference, 2004, London, at Hhttp://www.openwave.com/us/events/anti-abuse london/H.

- ⁵⁵ M. Prince presentation at MIT Spam Conference webcast, online at: Hhttp://spamconference.org/H.
- ⁵⁶ See Intel sees big changes to the net, online at Hhttp://news.bbc.co.uk/1/hi/technology/3643902.stmH.
- David Farber, see "Gates: Buy stamps to send e-mail: Paying for e-mail seen as anti-spam tactic", CNN, 5 March 2004, online at: Hhttp://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/H. See also "Make 'em pay", The Economist, 14 February 2004.
- ⁵⁸ See "Developing countries and spam" contribution to the ITU WSIS thematic meeting on countering spam, online at: http://www.itu.int/osg/spu/spam/contributions/Developing%20countries_contribution.pdf
- ⁵⁹ See note 48.
- ⁶⁰ See EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and EU Directive 2002/58.
- ⁶¹ For problems related to the utilization of SMTP, see FTC "National Do Not Email Registry: A Report to Congress", June 2004. "See D. Sorkin, supra note 47.
- ⁶² J. Magee, note 15.
- 63 See: Hhttp://www.ftc.gov/opa/2004/04/adultlabel.htmH.
- ⁶⁴ Under "Mandatory Indication of Advertisement". See: Hhttp://www.spamcop.or.kr/eng/m 2.htmlH.
- ⁶⁵ The same problem arose in the US before the creation of a federal anti-spam legislation. Different states in fact enacted conflicting label schemes. See D. Sorkin, "Technical and legal approaches to unsolicited electronic mail", University of S. Francisco L. Rev. (2001),
- ⁶⁶ On the different approaches to privacy and treatment of personal data in the Internet environment in Europe and US see, for example "The EU privacy directive and the resulting safe harbour: The negative effects on US legislation concerning privacy on the Internet" Vanderbilt Journal of Transnational Law, Vol. 35, 2002.
- ⁶⁷ See J. Magee, note 15.
- 68 D. Sorkin, *supra* note 65.
- ⁶⁹ In this sense, Australia signed, back in 2003, a MoU with Korea on cooperation in fighting spam, and more recently, on 2 July 2004, authorities from the United States, United Kingdom and Australia signed another Memorandum of Understanding on Mutual enforcement assistance in commercial email matters. Online at Hhttp://www.ftc.gov/os/2004/07/040630spammoutext.pdfH.
- ⁷⁰ In 1998 AOL successfully sued CN Production claiming the unauthorized use of the AOL trademark in the e-mail header constituted trademark infringement. See AOL v. CN Production, Civil Action, No 98-552-A, 1998.
- 71 See J. Magee, "The law regulating unsolicited commercial e-mail: an international perspective", Santa Clara Computer and High Technology Law Journal, May 2003.
- Note that the case CompuServe v. Cyberpromotions, the judge retained that violation of personal property can be committed by "intentionally using or intentionally bringing about a physical contact with the chattel in possession of another".
- ⁷³ D. Sorkin, *supra* note 65.
- ⁷⁴ See J. Magee, *supra* note 14, and M. Geist, supra note 49.

⁵³ IETF Message Transfer Authorization Records in DNS (marid) Working Group, online at: Hhttp://www.ietf.org/html.charters/marid-charter.htmlH; see also "IETF to lead anti-spam crusade", 12 April 2004, online at: Hhttp://www.nwfusion.com/news/2004/0412marid.htmlH

⁵⁴ The FTC in its last report to the congress considers the establishment of an authentication standard a must. See FTC National Do Not Email Registry A Report to Congress, Hhttp://www.ftc.gov/reports/dneregistry/report.pdfH . ISPs are also trying to put together their approaches, cooperating in the implementation of a single mechanism.

- ⁷⁶ "Primer caso judicial contra el spam en la Argentina", Wired News, 21 November 2003. Online at: Hhttp://gt.wired.com/wired/negocios/0,1154,25501,00.htmlH.
- ⁷⁷ Fraud is generally considered a criminal offence and defined as an act committed knowingly by a person who by deceit, falsehood or other fraudulent means defraud any person of a property or money.
- ⁷⁸ In Europe, misleading advertising is illegal under Directive 84/450/EEC, later amended to specifically deal with consumers' protection and unfair commercial practices. See European Commission Communication on unsolicited commercial communications or 'spam'.
- ⁷⁹ The Commission brought to court 62 cases in which spam was an integral element of deceptive and unfair practice, and therefore a violation of FTC Act Sect. 5. See FTC Report to Congress on Do Not Spam Registry, and H. Stevenson, OECD Workshop on spam, online at Hhttp://www.oecd.org/dataoecd/3/31/26991168.pdf H and M. Geist, supra note 49.
- ⁸⁰ In fact, the MoU with Australia and United States was signed by three UK entities: The UK Office of Fair Trading, the UK Information Commissioner, the Secretary of State for trade and industry. See Operation Secure Your Server, Ofcom webpage at: Hhttp://www.ofcom.org.uk/ind_groups/ind_info/telecoms/osys/?a=87101H. Secure your server homepage Hwww.ftc.gov/secureyourserverH.
- ⁸¹ See FTC Report to Congress: according to one ISP's litigation, costs range from USD 100,000 or less to more than USD 2 million when the spammer mounts an aggressive defence.
- 82 M. Prince "How to Craft an Effective Anti-Spam Law", June 2004, online at Hhttp://www.itu.int/spamH.
- 83 "Suing the Pants Off Spammers", Wired News, May 2004, online at: Hhttp://www.wired.com/wired/archive/12.05/view.html?pg=3H On technical collaboration, see "Anti-Spam Technical Alliance Technology and Policy Proposal", Anti-Spam Technical Alliance (ASTA), 22 June 2004, online at Hhttp://download.microsoft.com/download/2/3/7/23779c05-d409-46ce-b9d6-c24908789d8b/ASTA%20Statement%20of%20Intent.pdfH.
- Information commissioner webpage "What is the Government doing about spam?" Online at: Hhttp://www.informationcommissioner.gov.uk/eventual.aspx?pg=SR&cID=5809H.
- ⁸⁵ The text is available online at Hhttp://www.ftc.gov/os/2004/07/040630spammoutext.pdfH.
- 86 See contribution from the ACA to the ITU WSIS meeting on countering spam, "Multi-lateral and bi-lateral cooperation: the Australian approach", by J. Haydon, online at:
 Hhttp://www.itu.int/osg/spu/spam/contributions/John%20Haydon_ACA_Multilateral%20and%20Bilateral%20Cooperation.pdfH.
- 87 Online at: Hhttp://www.aca.gov.au/consumer info/frequently asked questions/spam MOU.rtfH.
- ⁸⁸ Communication from the Commission on unsolicited commercial communications or "spam", COM (2004) 28 final.
- ⁸⁹ EC COM(2004)28 final p.18-19.
- 90 Held on 22 April 2004. See EU Presidency News Summary online at Hhttp://www.ue2004.ie/templates/news.asp?sNavlocator=66&list_id=607H
- ⁹¹ See: "Transactions conducted online are expected to be worth EUR 2.2 trillion in the EU by 2006", 22 April 2004, Hhttp://www.eu2004.ie/templates/news.asp?sNavlocator=66&version=printerfriendly&list_id=593H.
- ⁹² Virtual conference on regulatory cooperation on spam, online at: Hhttp://www.itu.int/ITU-D/treg/Events/Seminars/Virtual-events/Spam/index.htmlH.
- 93 Information regarding the meeting outcome and future work on countering spam are available at: Hhttp://www.itu.int/spamH.
- 94 Available at Hhttp://www.itu.int/osg/spu/spam/law.htmlH.

Note That the Primo Piano/Cronache/2004/06 Giugno/24/spamming.shtmlH.
75 See EU Directive 95/46/EC. Recently an Italian judge condemned a company that sent unsolicited commercial e-mails to several thousand people, recognizing that spam can cause economic damage to the recipient. The case was brought to court by a consumer association, and the judgement has been taken on the basis of the Italian law protecting privacy. See "Spamming, prima sentenza di risarcimento danni", online at:

- ¹⁰⁰ Howard Beales, Director of the FTC's Bureau of Consumer Protection, online at: Hhttp://www.ftc.gov/opa/2004/01/opsecure.htmH.
- 102 Hhttp://www.icpen.org/H.
- 103 Hhttp://www.econsumer.gov/H.
- 104 See the ITU WSIS Thematic Meeting on Countering Spam webpage on international cooperation at: Hhttp://www.itu.int/osg/spu/spam/intcoop.htmlH.

⁹⁵ See Telecommunication Standardization Advisory Group (TSAG) online at: Hhttp://www.itu.int/ITU-T/tsag/index.aspH.

⁹⁶ ITU WSIS thematic meeting on countering spam, Chairman's report, online at http://Hwww.itu.int/spamH.

⁹⁸ The topic of spam was proposed by Canada.

⁹⁹ Asia-Pacific Economic Cooperation, Electronic Commerce Steering Group (APEC-ECSG), online at: Hhttp://www.apecsec.org.sg/content/apec/apec_groups/som_special_task_groups/electronic_commerce.htmlH.