COMBATING SPAM THROUGH LEGISLATION: A COMPARATIVE ANALYSIS OF US AND EUROPEAN APPROACHES

Evangelos Moustakas
School Of Computing Science
Middlesex University
London, NW4 4BT, UK.

Prof C. Ranganathan
University Of Illinois At
Chicago, 601 S Morgan Street,
Chicago, IL-60607, USA

Dr. Penny Duquenoy
School Of Computing Science
Middlesex University
London, N14 4YZ, UK.

.

Abstract

Unsolicited Commercial Communication - also known as spam - has traditionally been the most visible e-mail threat and has reached a point where it creates a major problem for the development of e-commerce and the information society. It is currently estimated that 60 per cent of all e-mail messages are spam. The United States, Australia, Canada, European Union including the United Kingdom have all recently implemented legislation in an attempt to combat Unsolicited Commercial Communication (UCE). However due to the difficulty and complexity of the problem the implementation and enforcement of the law in a global environment is still to be resolved. This paper provides an overview of the various laws relevant to the problem of spam, and compares United States and European Union anti-Spam Legislation. It examines the extent to which law addresses the problem of spam and discusses some weaknesses.

1 Need for anti-spam Legislation

Spam is just the tip of the 'cyber-crime' iceberg (Jean-Jacques Sahel, 2005). The increasingly sophisticated variants of spam and the threats they pose have brought anti-spam measures to the forefront of attention of several governmental agencies, consumer groups and business cohorts worldwide. According to Erkki Liikanen, European Commissioner for Enterprise and the Information Society: 'Combating spam has become a matter for us all and has become one of the most significant issues facing the Internet today'. Unsolicited Commercial Communication has reached a point where it threatens the future development of e-commerce and the information society. Spam not only impinges on the privacy of individual Internet users but also creates economic losses and as well as time-related losses in terms of the time spent reading and deleting the messages (European Commission Report, 2003). Spam assists cyber-crime (Tony Dearsley, 2004) and poses a threat to consumer confidence in e-commerce. A significant proportion of spam contains fictitious information about the sender, misleading subject lines and extravagant earnings or performance claims about chain letters, pyramid schemes, advertisements for pornographic web sites, 'quack' products and remedies, and illegally pirated software. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of Internet etiquette (Vint Cerf, 2002).

Further, spam also burdens the ISPs who bear much more of the cost of providing the infrastructure than the sender does including the need to pay for extra storage and bandwidth. Because of spam, ISPs also face the ire of their customers who perceive spam as a consequence of poor service levels and performance issues of the ISP (Wall, 2004). Several systems have collapsed due to the sheer bulk of spam. Table 1 below provides an overview of the problems associated with spam.

Spam affects a diverse range of stakeholders ranging from customers, small and medium sized businesses to larger corporations and even governmental agencies. Given the severity of the issue and the potential damages spam can cause, legislative measures have been suggested to control and possibly eliminate spam. Spammers may not be affected by anti-spam legislation since they could change their tactics or simply move their servers to locations that that have not passed anti-spam regulations. However, action against spammers is not totally impossible. According to *Spamhaus (*an independent network which tracks Internet's Spammers, Spam Gangs and Spam Services), 80% of spam received by Internet users in North America and Europe is sent by a hard-core group of less than 200 spam

outfits, comprising some 500-600 professional spammers (Spamhaus, 2004). Therefore, it is possible to identify and control this core group of spammers. By effectively deploying legislative tools, it might be possible to penalize, control as well as minimize the spam groups.

Table 1: Problems association with Spam

Cyber Community	Problems associated with spam
Customers	- Spam impinges on the privacy of individual Internet users - 'E-mail harvesting' collects bulk e-mail addresses - E-mails usually contain malicious programming code that harms the computer or network - Stealing of critical customer information such as credit card information - Phishing scams (forged identities)
Employees and Corporations	- Time spent reading and deleting the messages - Additional cost for time-based connection fees - Lost productivity
ISPs	- Cost for providing the anti-spam infrastructure - Cost of extra bandwidth and storage to cope with the volume of spam - Poor performance levels (bandwidth) - Operating Systems have collapsed due to the volume of spam - Customer's dissatisfaction
E-Commerce environment	- Depletion of consumer confidence and trust - Extravagant earnings - Quack products undermine credibility of genuine ones - Illegally pirated software and other digital products
Governmental Agencies	- Violation of netiquette - Spam can be offensive / Pornographic material – violating laws

2 A review of anti-spam Legislation

Given the global reach of the Internet, most Governments have avoided interfering in Internet issues preferring to allow the system to regulate itself. However, the evasive and pervasive nature of spam has forced governmental bodies to deal with the problem. Nations have enacted different kinds of laws and have enacted varied legislations to control spam. Table 2 below provides an overview of the anti-spam legal environment in the European Union, Australia, Canada, USA, Japan and New Zealand.

Table 2: Anti-spam legal environment

Country	Legislation – Anti-spam Statutes
Australia	- Spam Act of 2003 - Telecommunications Act of 1997 - Australia Parts IVA, V, and VC of the Trade Practices Act of 1974
Canada	- Personal Information Protection and Electronic Documents Act (PIPEDA) - Competition Act. - Charter of Rights Freedoms - The Criminal Code and the Competition Act - Canadian Code of Practice for Consumer Protection in E-Commerce
EU	- Privacy and Electronic Communication Regulations 2003 (UK) - Data Protection Act of 1998 (UK) - Electronic Commerce Regulations of 2002 (all adapted from EC Directives, e.g. Directive on Privacy and Electronic Communications 2002/58/EC)
Japan	- The Law on Regulation of Transmission of Specified Electronic Mail July 2002 - Specific Commercial Transactions Law, 2002
New Zealand	- Has not yet enacted Legislation to regulate spam. In progress – in place summer 2005 tbc.

USA	- Can-Spam Act of 2003 - Laws enforced by the Federal Trade Commission - Section 5 of the Federal Trade Commission Act

The focus of this paper is to compare and contrast two of the major approaches that are in place to deal with spam. We specifically focus on the approaches of US and European Union. In the following sections we discuss two major pieces of legislation from the US and EU – the Can-Spam Act of 2003, and the EU Directive that informs UK legislation.

2.1 European Union and UK Legislation

2.1.1 Key elements of the EU Directive

In the European Union (EU) the negative effects of spam were recognized, however the question remained as to whether the sending of spam was a legitimate activity. UK Law (UK Legislation, 2003) largely follows the EU Directive (EU Directive - 2002/58/EC, 2002). In July 2002, the European Parliament and the Council voted to ban Spam. This directive specifies the following:

> *(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them.*

This directive means that people have to "opt in" or specifically place a request to receive commercial e-mail. Under Article 13 of the Directive, the use of e-mail and SMS (text message to mobile phones) for direct marketing will only be allowed in case of those customers /subscribers who have given their prior explicit consent. Such a directive places e-mail marketing on the same footing as unsolicited faxing and automated telephone systems. The term 'opt in' in receiving unsolicited commercial e-mail is expressed as *'for the time being'*. It is not specifically defined in the regulations but it implies that the consent has a transient nature and the Guidance makes clear that the consent will remain valid until it has been specifically withdrawn or it is otherwise clear that the recipient no longer wishes to receive marketing commercial communications.

> *(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC…….*

The Directive makes an exception where there is an existing customer relationship and the supplier has obtained the customer details in the context of a sale of goods or services. In this case, the supplier may use the customer details for the purpose of direct marketing in relation to its own similar goods or services.

> *(41)….. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.*

The customer must be clearly and distinctively given the opportunity to object, free of charge and in an easy manner, to the use of the e-mail address when collected and on the occasion of each message in case the customer has not initially refused such use. This exception leaves open to interpretation whether goods or services advertised are similar to those previously purchased. Moreover, it seems from the wording that the exception only applies where there has been an actual sale rather than for example an enquiry. It also appears that only the party that obtained the details can use them. For instance, a manufacturer cannot send e-mails to customers whose e-mail address was obtained by a retailer. The term 'similar products and services' is related to soft opt-in. That means that a product or service can be offered only during the negotiation period or if it is similar to those offered in the marketing e-mail communication.

> *(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes*

The Directive also prohibits sending direct marketing e-mails that disguise or conceal the identity of the

sender or are without a valid address to which the recipient may send a request that such communications cease.

2.1.2 Effectiveness of the EU Directive

Implementation Issues

The implementation of the EU Directive differs between the Member States. While some impose fines for unsolicited e-mail sent to both customers and businesses, others only penalise in the case of spam sent to customers. Also the term 'opt-in' is open for interpretation. More specifically some National Laws (e.g. Spain) had already introduced the 'opt-in' regime for e-mail before the Directive of 2002. Other National Laws transposed the Directive but 'modified' the concept of 'opt-in' (e.g. Denmark) and several Member States transposed the Directive only partially (e.g. Belgium). Finally, a large number of Member States transposed the Directive as late as in summer 2004 (e.g. France, Germany). Spain takes the view that messages can only be sent to those who have given their authorisation, but Denmark has banned the sending of messages unless the recipient has actually requested them. In the UK, participation in a draw would constitute consent to receive further e-mails. The Information Commissioner in UK notes that: 'Harmonisation among the Member States is the desirable objective but also a very difficult task' (Phil Jones, 2003).

Individual/Corporate Subscribers

There are a number of divergences between Member States such as: whether the Directive applies to natural and/or legal persons; whether the requirements for consent are oral/written, explicit/implicit, active/passive and who manages the opt-in/opt-out mailing lists. The distinction between individual and corporate subscribers is an important issue since the use of e-mail and SMS for direct marketing is only allowed in respect of subscribers who have given their prior explicit consent. The definition of 'individual' covers traders such as consultants who run their business on their own rather than under the umbrella of a company. When the recipient of commercial communication is a partnership subscriber the question is raised as to whose consent is required. Strictly speaking the Legislation states that the consent of the individual recipients or persons should be obtained. However, the UK Information Commissioner recognises that there are circumstances where the wish of the organisation to receive marketing materials, may override the wishes of individual employees. Therefore, marketers may obtain consent from a single person who acts on behalf of the partnership to receive commercial communication. Finally, marketers should ensure that they comply with the principles of the Data Protection Act 1998.

Which Law Is Applicable?

There are also practical questions that the EU Directive has not explicitly addressed such as which law is applicable if a UK-based company sends unsolicited e-mail to Italy and vice-versa. According to the UK Information Commissioner if both sender and recipient are companies, sending spam is not illegal. If the recipient is an individual he can complain to the sender's ISP or the Direct Marketing Association. The recipient in Italy may also sue the sender in UK and the court will take place in UK. Szabolcs Koppanyi (2003) of the European Commission agreed that the EU needs to find a common forum for exchanging views and explained that a process is being put in place within the European Commission for investigating the following elements of the Directive: Remedies and penalties, complaints procedures, cross-border complaints, co-operation with third countries, monitoring, contractual arrangement, codes of conduct, acceptable marketing practices and out-of-court redress. The European Contact Network of Spam Authorities (CNSA) was established for that purpose in 2004.

Transition Rules

Transition rules for adopting the new Legislation have often been left out creating a 'grey zone' for both companies and customers. Many legitimate companies use e-mail newsletters to communicate with their customers and in several cases this type of communication dates as far back as the 1980s. Since it is hard to prove which recipient has opted-in the question is if companies have the right to send a single e-mail message to existing subscribers to inform them that they must take action to confirm their subscription, or they have to stop all types of sending. In the event that they decide to stop all types of sending they could be faced with an avalanche of phone call requests from confused customers asking why they do not receive newsletters anymore.

2.2 USA Legislation – Can-Spam Act 2003

According to the United Nations Conference on Trade and Development (UNCTAD) 2003 e-commerce and development report, currently over 58% of all spam e-mail messages originates from U.S.A. Therefore, it is only natural that the US spam-related legislation is of considerable interest to the rest of the world. (UNCTAD, 2003) The US Bill was signed by the President on December 16, 2003, and took effect on January 1, 2004 (CAN-SPAM Act, 2003). The purpose of the Act is to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.

2.2.1 Key elements of the US Legislation

The Can Spam Act of 2003 represents a 'compromise' between the various spam stakeholders and allows e-mail marketers to send UCE until the consumer opts-out from receiving future messages. It also requires e-mail marketers to identify UCE as advertisements (ADV), as well as to include warning labels on UCE that contains sexual material.

Section 5

(a) Requirements for transmission of messages

(1) It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message …that contains…… header information that is materially false or materially misleading.

(2) Prohibition of deceptive subject headings …...

(3) Inclusion of return address ……

(5) Inclusion of Identifier, Opt-out, and physical address ……

The new law calls the Federal Trade Commission (FTC) to study the feasibility of a Do-Not-Spam List of e-mail addresses and prohibits spammers from disguising or hiding their identities. Spammers are also barred from harvesting addresses from web-sites and must include an opt-out option in their messages. It also requires that commercial e-mail should include the sender's valid physical address and recipients must be given an opt-out method. Convicted spammers could face penalties of up to five years in prison.

(A) It is unlawful for any person ……

(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website ……

(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations.

Can-Spam prohibits address harvesting and dictionary attacks. Many spammers use automated software to collect e-mail addresses through the internet by searching web-sites, newsgroups, mail lists or other on-line resources that could possibly contain e-mail addresses.

(2) to use scripts or other automated means to register for multiple electronic mail accounts

(3) to relay or retransmit a commercial electronic mail message …… without authorization

The Can-Spam Act makes it illegal to use automated techniques such programming scripts to sign up for e-mail accounts for the purposes of sending unsolicited commercial e-mails.

S. 877—6

(b) PENALTIES — the punishment for an offense under subsection

(a) is (1) a fine under this title, imprisonment for not more than 5 years, or both, if—

''(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

''(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

''(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

''(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

''(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

The US anti-spam Law makes it a crime (SpamLaws, 2003), subject to five years imprisonment, to send fraudulent e-mail using standard spam tactics as false headers and misleading subject lines and provides for civil penalties up to $11.000 per violation (CBC News, 2004). Additionally the Congress gave the FTC a list of tasks such as issuing a regulation requiring that any spam containing sexually oriented material must include the warning "SEXUALLY-EXPLICIT" in the subject line.

2.2.2 Can 'Can-Spam Act' reduce spam?

Positive Impact

The Can-Spam Act set out to reduce unsolicited e-mail by targeting the fraudulent use of third party computer systems to relay e-mail messages, as well as messages that are unsigned or have fraudulent return addresses. It also requires all e-mail messages to include opt-out functions. The Act will indeed assist in some way to tackle the problem of spam. It makes illegal the use of open proxies or the use of false headers. To circumvent legislation, US spammers will now have to send out emails from their own identifiable IP addresses, rather than steal 3rd party relays and proxies.

You Can Spam; Just Do Not Use False Headers!

However the new US law may not entirely stop spam. As described above, the Legislation takes an opt-out approach. The big concern regarding the opt-out mechanism is that it gives the right to spammers to send spam. That means that corporate IT managers are going

to keep the anti-spam filters at the mail gateway, blocking the flow of now legal but still unsolicited emails (Cameron Sturdevant, 2003). Several negative comments were addressed at the 'Spam and the Law' conference in San Francisco on January 22, 2004 about the effectiveness of the Federal Can Spam Act. Many professionals in the technical and legal areas have questioned the federal government's ability to enforce those restrictions and have criticized the way the act supersedes stricter state laws (Amit Asaravala, 2004).

Do-Not Spam Registry

Regarding the national do-not spam registry, the FTC Chairman Timothy Muris during a press conference in June 2004 stated that without an effective system for authenticating the source of email, any efforts to develop a registry of individual e-mail address will fail (Bill Grabarek, 2004). Most spammers who already violate the anti-spam laws would ignore the requirements not to send unsolicited commercial communication to e-mail addresses that are in a do-not-spam database. Spammers might even use the do-not-spam registry as a source of valid email addresses to spam further (Gary D. Halley, 2004).

Enforcement Issues

Since Law is only as good as its enforcement, no change can be seen in the level of spam until enforcement happens. Though the new Legislation has been gradually enforced in all the 37 US States, it overrides more strict spam punishments set by some states. In California, for example, Sen. Debra Bowen's bill would have cost spammers $500 per unsolicited e-mail. The new federal anti-spam bill may not be as effective for California or Delaware, which were closer to developing a more effective anti-spam legislation. Both California and Delaware had specified that bulk commercial communication could only be sent to recipients who had opted-in to receive it. Also, California's law would have provided a way for individuals to sue offenders. The Federal Legislation does neither of these things since it is only up to the Government agencies and ISPs to pursue spammers. Unfortunately, the Federal Legislation will create a kind of bulk unsolicited commercial e-mail that is legal under their own rules.

3 Legal recommendations to combat spam

Legislation alone will not result in an immediate or dramatic reduction of the spam, but it is an important element of the framework both in practice and perception. Moreover, a well developed law can distinguish between good actors and bad actors and decide penalties accordingly. In order to implement effective legislative measures, Governments should also consider an information campaign on spam issues that will target users, business communities, private sector groups and other Governmental bodies. The goals of Anti-spam Legislation are first to reduce and finally combat illegal spam; and secondly, to guarantee a secure e-commerce environment for consumers and organisations. Effective legislation would give the recipients of spam, both individuals and corporations, the ability to go against the offensive spam users and businesses that use deceptive techniques to forge e-mail headers, harvest e-mail addresses and send bulk mailings that people do not want.

3.1 Effective Use of Advances in Information Technology

Lack of trust, security and harmonised national legislation, in addition to an increasing number of reported cyber-crimes, viruses, spam and fraud have become major threats to the development of e-commerce. Providing an enabling legal framework is a fundamental element for the development of e-commerce, as it particularly affects the ability to conduct transactions online. Although it is well known that commerce and technology often advance ahead of the law and that historically the law has adapted to serve commercial and financial demands and facilitate trade, it is equally true that technology needs to take into account relevant legal requirements. Furthermore, efficient regulation of e-commerce issues such as spam and digital rights management requires that legislative solutions be accompanied by technical solutions (United Nations E-Commerce and Development Report Chapter 3, 2003). Spam is just a sample of the vulnerability of the Internet Infrastructure. The anti-spam solution involves also updating the e-mail system so that spammers will not be able to hide the origins of their e-mail messages. The key technical element for that is authentication. With increased focus on authentication, better understanding and enforcement of the Anti-spam Legislation, the problem of spam can be tackled. If spam can be stopped at the identity level and spammers start to fear the criminal and civil penalties, then the problem of spam may be alleviated. The real challenge of legislation is to define what constitutes proof that a communication was unsolicited. Due to the insecure nature of the SMTP protocol even records of a double opt-in confirmed subscription can be easy to fake and as a result unreliable as proof. One of the challenges for Legislation is to go after spammers and make sure that they are not companies that use legitimate methods to send commercial e-mail communication. With laws that allow an individual to take private action an individual might sign-in to a list and then claim to be spammed.

3.2 Penalties and Enforcement

In order for anti-spam Legislation to be effective, it must define penalties that are sufficient to act as a real deterrent, and it must allow actions and enforcement to occur in a forum or court accessible to the majority of victims. Additionally, if the anti-spam Law requires action to be taken in the regular court system of most countries, then the costs of simply bringing the action to court will prevent most cases, since the cost will be high. As a result, it is important for anti-spam legislation to allow victims to bring their complaints to the forum or court in an easy and cost effective way.

3.3 International Co-operation among the Legislative Bodies

The problem of spam is fundamentally an international problem, which can only be fully addressed through international co-operation and coordinated action (Philippe Gerard, 2005). The Governmental bodies need to continue to participate and actively contribute to international anti-spam initiatives. Clearly one of the biggest problems with legal remedies is the number of jurisdictions involved which leads to the conclusion that the need for co-operation by legislators is essential. Anti-spam Legislation could be considered a way to prevent spam, but most of all, as a tool to punish spammers after they are identified. Arresting some of the spammers will not stop spam, but it will contribute to the reduction of spam in the future. An example of international anti-spam co-operation is the tripartite Memorandum of Understanding on Spam enforcement cooperation, an agreement between the UK, United States and Australia in order to combat the problem of spam (Department of Trade and Industry, 2004). This will mean that enforcement authorities in the UK, United States and Australia will work together to investigate spammers in those countries, as well as join training initiatives to combat spam. International solutions and strengthening capabilities will be developed to trace and convict spammers and cross border enforcement against spammers will take effect.

Another co-operative agreement is the 'London Action Plan' an international action plan that has been agreed by 19 bodies from 15 countries and which objective is to communicate and co-operate on enforcement action to tackle spam (Office of Fair Trading 'London action plan on spam', 2004). The London Action Plan aims to develop international links to address spam and spam-related problems. Among others the London Action Plan encourages communication and coordination between agencies to achieve efficient and effective enforcement and discuss cases, legislative developments, investigative techniques, ways to address obstacles to enforcement, consumer and business education projects, to promote ways to support government agencies in bringing spam cases and pursue their own initiatives to fight spam.

Finally, the Organisation for Economic Co-operation and Development have set up a task force to marshal the efforts of government, business and civil society in order to tackle the problems posed by unsolicited e-mail messages, or spam (OECD Work on Spam, 2004). Key objectives of the OECD will include coordinating international policy responses in the fight against spam, encouraging best practices in industry and business, promoting enhanced technical measures to combat spam along with improved awareness and understanding among consumers, as well as facilitating cross-border law enforcement.

3.4 Global Harmonisation in Anti-spam Legislation

The legal framework is a key element in the e-commerce environment that affects market participation. It is important to hold a broad public dialogue and debate with all anti-spam stakeholders before preparing e-commerce legislation, so as to ensure fairness and an equitable balance between different interests at stake (United Nations E-Commerce and Development Report Chapter 1, 2003). There can be no solution to the spam problem without some kind of worldwide ‘minimum standard’ of legislation. Global harmonisation is a very difficult task since US and EU have opt-out / opt-in regimes. Despite this variation, in the future we may see that the requirements for sending Commercial Communication around the world will be similar. For example, when the e-mail contains pornographic material only a URL link should be included in the body of the message and in addition the subject line of the e-mail should inform that the message is pornographic.

3.5 Silver bullet? - Need for United Approach

There is no single solution or silver bullet that can be sufficient enough by itself to tackle the problem of spam. As a result, the solution to the problem of spam will be a combination of laws and technology that effectively will combat spam. Even if the anti-spam Legislation was effective, Law itself is not sufficient to tackle the problem of Spam. Different stakeholders (ISPs, Marketing Associations etc) need to co-operate to find an integrated solution to handle spam. According to Commissioner Liikanen an OECD framework (OECD, 2004) should aim to promote:

- An effective ‘anti-spam’ law in all countries;
- *Cross-border cooperation* on enforcement in specific cases;
- *Self-regulatory solutions* by market players e.g. on contractual and marketing practices;
- *Technical solutions* to manage or reduce spam, like filtering and other security features;

- Greater *consumer awareness* about, e.g., how to minimise spam and how to react to spam and complain.

Conclusions

Spam accounts for half of all worldwide email and is expected to continue to grow. It is a real and costly threat to the communications infrastructure that we increasingly rely on for social, business-related and employment purposes. In this paper, our goal was to highlight how legislative approaches can help combat spam, and specifically compare and contrast the legislative approaches in US and UK (EU). As argued earlier, anti-spam legislation addresses certain problems such as intrusion of subscriber's privacy by unsolicited communications for direct marketing purposes, as well as provides clear instructions for false identities or false return addresses. However, a lot more work still needs to be done in order to tackle the problem. .Legislation in isolation will not be able to eliminate spam. What is needed is a united approach, complemented by effective enforcement mechanisms, cross border co-operation, consumer and industry education, coupled with effective implementation of advanced technical solutions. The co-operation between anti-spam groups, legislation bodies and advisory councils, direct marketing groups, and ISPs, and a joint-coordinated action involving all these groups is the most effective way to combat and eliminate spam.

Acknowledgments

The authors would like to thank the anonymous reviewers as well as Jean-Jacques Sahel for their valuable feedback.

References

Jean-Jacques Sahel (2005). 'Spam as a vehicle for transnational criminal menace' ASEM London 4th Conference on eCommerce Tackling Spam. [http://www.asemec-london.org]

Dr. David S. Wall (2004). 'Can we can the spam?' Director of the Centre for Criminal Justice Studies at the School of Law, University of Leeds Computers and Law February – March 2004 Vol. 14 Issue 6

Tony Dearsley (2004). Computer Investigation Manager, Vogon International 'Computer and Internet Crime Conference/Exhibition

Vint Cerf (2002). Senior Vice President, MCI and acknowledged "Father of the Internet" "Spamming is the scourge of electronic-mail and newsgroups on the Internet. Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization."

Spamhaus (2004) 'SBL Blocklist Rationale' [http://www.spamhaus.org/sbl/sbl-rationale.html]

UK Anti-spam Law: Consumer Protection (Unsolicited E-mails) (2003) [http://www.parliament.the-stationery-office.co.uk/pa/cm200203/cmbills/119/2003119.htm]

Directive 2002/58/EC of the European Parliament and of the Council (2002).

Szabolcs Koppanyi (2003) European Commission UK EEMA Conference Dublin

United Nations Conference on Trade and Development (2003) E-commerce and Development Report [http://www.unctad.org/en/docs/ecdr2003ch1_en.pdf]

CAN-SPAM Act (2003). Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 Senate

Cameron Sturdevant (2003). 'Anti-spam law has holes' eweek December 8, 2003 p 54.

Amit Asaravala 'With This Law, You Can Spam' [http://www.wired.com/news/business/0,1367,62020,00.html] (January 23, 2004)

Bill Grabarek (2004) Direct Newletter 'FTC: DO-Not-Spam Not the Answer'

Gary D. Hailey (2004). 'Congress Urges FTC to Crack Down on Spammers' Legal Review – Response Magazine

United Nations Conference on Trade and Development (2003). E-Commerce and Development Report 2003 Internet edition prepared by the UNCTAD secretariat Chapter 3: ICT strategies for development. [http://www.unctad.org/en/docs/ecdr2003ch3_en.pdf]

Philippe Gerard (2005). 'Co-operating internationally against spam' - ASEM London 4th Conference on eCommerce Tackling Spam.

Department of Trade and Industry (2004). Global trio Forge anti-spam Pact [http://www.gnn.gov.uk/environment/detail.asp?ReleaseID=121897&NewsAreaID=2&NavigatedFromDepartment=True]

Office of Fair Trading (2004). 'London action plan on spam' [http://www.oft.gov.uk/News/Press+releases/2004/168-04.htm]

OECD Work on Spam (2004) [http://www.oecd.org/sti/spam/]

United Nations Conference on Trade and Development (2003). E-Commerce and Development Report 2003 Chapter 1: Recent Internet trends: Access, usage and business applications [http://www.unctad.org/en/docs/ecdr2003ch1_en.pdf]