Information & Communications Technology Law,
Vol. 16, No. 1, March 2007

Anti-Spam Legislation: An Analysis of Laws and Their Effectiveness

GUIDO SCHRYEN

Institute of Business Information Systems, Aachen University, Germany

ABSTRACT *More than half of worldwide e-mail traffic (an estimated total of several billion e-mails per day) consists of spam. This is becoming a considerable disturbance to telecommunications. Spam is also closely related to other kinds of cybercrime as it possibly contains malicious software or is pursuing some kind of fraudulent aim such as phishing. As well as technical and organizational measures, many countries have introduced anti-spam legislation. However, today's worldwide legislative coverage of spam is heterogeneous, and its effectiveness is discussed controversially. This article describes important parameters by which anti-spam legislation can vary and gives an overview and analysis of worldwide anti-spam legislation, including the European Directive 2002/58/EC and the United States CANSPAM Act 2003, and international cooperation, such as the London Action Plan. The article then proceeds to discuss the effectiveness of current laws and identifies problems resulting from the fact that an international phenomenon is being addressed by national legislation. Finally, the article presents suggestions for overcoming some of these problems.*

Introduction

Spam has become a considerable disturbance to telecommunication. This disturbance influences many communication services, including both mobile services (e.g., SMS or MMS) and Internet services (e.g., instant messaging, the Usenet and e-mail). Spam e-mails, which are the focus of this article, are regarded as a violation against Internet etiquette and are closely related to other kinds of cybercrime: Spam e-mails may contain malicious software (e.g., Trojan horses, viruses and worms). Furthermore, they may have the intention of phishing, and amount to a 'Denial of Service' attack, if they overfill an e-mail postbox.

Although spam is often defined as 'unsolicited bulk e-mail' (Spamhaus, 2006a), it is still a fuzzy term. Until a precise and operational definition of what 'unsolicited' and 'bulk' mean is available, any classification of an e-mail as 'spam' will remain a subjective one. This subjective understanding of spam may flow into assessment tools of Internet Service Providers (ISPs) and other spam-recording organizations, both of which measure the portion of spam. Although the percentages vary, spam usually makes up about 60% of all e-mails sent (Commtouch, 2006; MessageLabs, 2006). The market research company IDC estimates that, in 2006, the total number of e-mail messages sent daily exceeded 60 billion worldwide, resulting in a huge demand for storage capacities and

ISSN 1360-0834 print/ISSN 1469-8404 online/07/010017–16 © Taylor & Francis
DOI: 10.1080/13600830701194521

bandwidth. Many other problems are associated with spam (Moustakas et al., 2005), so that it is not merely a cumbersome annoyance, but has even become an economic burden to e-mail stakeholders. The economic damage caused by spam emails is estimated at several billion American dollars (OECD, 2003; EU, 2001). Given this severity and the potential damages that spam can cause the European Union (EU) and the authorities of many countries and federal states have started to address spam through legislation. Although laws and regulations have not led to any substantial decrease in spam yet, other kinds of measures (e.g., technical and organizational ones) have not succeeded to any great extent either. They are, however, promising in several ways:

- They provide clear legislative guidelines for companies, thereby restricting reputable companies' uncontrolled e-mail marketing (Sester & Mutschler, 2006).
- If it is true that most of the spam targeted at Internet users in North America and Europe is generated by a hardcore group of known professional spammers whose names, aliases and operations are documented in the Spamhaus Register of Known Spam Operations (ROKSO) database (Spamhaus, 2006b), then the prosecution of a small number of spammers would be likely to reduce spam enormously, provided that these come under an anti-spam jurisdiction.
- Legislation can help to limit the occurrence of spam by determent through impending penalties and through successful prosecution against spammers.

As no silver bullet against spam has yet been found, this problem would seem to need a multifaceted approach. Anti-spam legislation is meant to work complementarily to organizational, behavioral, technical and economic measures (Moustakas et al., 2005, p. 7).

Organizational measures comprise abuse systems that are intended to help the Internet community report and control network abuse and abusive users. Ideally, spammers are identified and duly prosecuted. Organizational measures also include forms of international cooperation such as bilateral government-to-government cooperation, cooperation between private sector groups, government-to-private sector cooperation and multilateral cooperation. These are discussed below.

Behavioral measures aim at e-mail users' procedures in using and distributing their e-mail addresses and dealing with any spam e-mails that they receive. Locations and services that seem to deserve protection are: newsgroups, mailing lists and newsletters, webpages, chat services and chat rooms, and address books and e-mails residing on users' hosts (Raz, n.d.). Many approaches have been proposed for protecting e-mail addresses from being harvested, including the usage of throw-away e-mail aliases and address obscuring/obfuscating techniques such as virtual channels (Hall, 1996), extended e-mail addresses (Gabber et al., 1998) and single-purpose addresses (Ioannidis, 2003). These approaches may help obscure addresses as long as spammers' harvesters are not trained to deal with the most frequently deployed hiding techniques. However, they are of limited use where e-mail addresses cannot be obscured arbitrarily.

A vast set of technological anti-spam measures, including the implementation of economic measures, has been proposed and deployed. This set includes, but is not limited to: IP blocking (a server decides to accept or reject an e-mail on the basis of the IP address of the e-mail client), filtering (a server classifies an e-mail as spam or

ham on the basis of e-mail content and/or IP connection data) and authentication (Myers, 1999; Leibzon, 2005).

Economic (payment-based) approaches, which are currently rarely deployed, rely on e-mail systems to create economic disincentives to spam. To accomplish this, e-mail servers require a small payment in exchange for delivering an e-mail to the recipient's inbox or for accepting an e-mail from a user client. The payment is kept small enough to allow legitimate e-mail to pass into user inboxes, but large enough to make the sending of large numbers of e-mails unprofitable or too time-consuming (Tompkins & Handley, 2003). However, at the same time, this poses the problem of how to deliver solicited bulk e-mail. The mode of payment could be CPU (computer processing) time (Dwork & Naor, 2002; Back, 2002) or memory capacity (Abadi et al., 2003; Dwork et al., 2003) as well as currencies. The proposals based on currencies typically require senders of e-mails or sending organizations to pay a fee for each e-mail communication, unless the recipient has whitelisted the sender. The currency used can be real cash (bonding schemes where the sender posts a bond to a third party that the sender forfeits if he or she spams) (Fahlmann, 2002; Loder et al., 2004; Templeton, n.d.) or virtual/digital cash (Turner & Havey, 2004).

Today's worldwide legislative coverage of spam is heterogeneous. While some countries have not introduced any anti-spam legislation at all, others have arrived at some degree of legislation. However, the existing laws differ in regard to several parameters, which are discussed in the next section. Core issues of the anti-spam legislation of 47 countries are then presented. International cooperation, which is intended to support domestic prosecution, is also covered. The present legislation landscape is then assessed in terms of effectiveness, currently unsolved problems are identified and means by which some limitations might be overcome are indicated. The article concludes with a summary.

The parameters of anti-spam legislation

Important parameters by which anti-spam legislation can vary are: the type of subscription, the scope, the sender and recipient type, and the set of possible accusers. Figure 1 illustrates the described parameters and their possible values.

Subscription

Laws can differ in the way in which a recipient can refuse to accept the receipt of e-mails; in other words, in the kind of subscription. There are two families of approaches: an 'opt-in' approach, which requires that the sender has the recipient's permission prior to sending, and an 'opt-out' approach, which provides a mechanism for declining the receipt of further e-mails from a particular sender. These families comprise the following provisions (Allman, 2003), which are presented in order of decreasing restriction on the sender's options.

- *Double opt-in*, which is sometimes also referred to as 'verified opt-in' or 'closed loop opt-in', requires that a subscriber takes two actions to get onto a list. The first action requests the addition of an e-mail address to a list and the adding-on can be done, for example, via a web form or an e-mail. The owner of the list then sends a confirmation (challenge) message, which must be answered by the recipient. Only when this reply is received is the address added to the list.

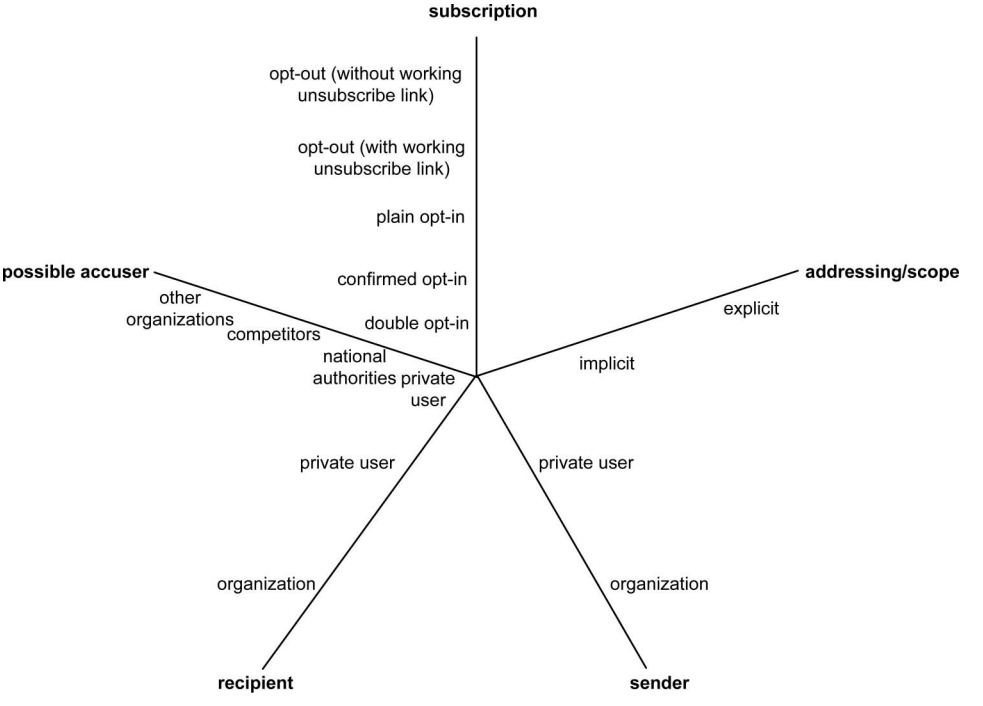

Figure 1. Parameters by which anti-spam legislation can vary.

The reason for requiring the sender to confirm the adding-on is that someone other than the address holder could have added the address without the permission of the holder.

- *Confirmed opt-in* works exactly like double opt-in, except that the confirmation message has to be answered or some other action has to be taken by the recipient in order to unsubscribe. For the sender, a problem with this approach occurs if, by law, it is the sender's obligation to prove that the recipient has explicitly accepted the receipt of e-mails.
- *Plain opt-in* does not include any kind of confirmation. Once an e-mail address is entered, it is added to the list, even if the address-holder has neither been involved nor has given consent.
- Generally, *opt-out* means that a sender may receive an e-mail without having given permission in advance, but being provided with a working unsubscribe link or an e-mail address that can be used for the cessation of the e-mail communication. Some countries, such as the United States (FTC, 2004), propose the maintenance of an address list that contains the e-mail addresses of consumers who do not want to receive commercial e-mails. Such a registry is called a 'Robinson list'. 'Opt-out' can also come with a nonworking unsubscribe link, or even with an unsubscribe link that actually confirms an address as belonging to a live account. These options usually play no role in legislation.

Scope

Anti-spam laws either explicitly or implicitly are directed against the sending of particular kinds of e-mails and the related harm they can cause. This kind of

addressing depends on the law's scope, which can cover, for example, (bulk) e-mails explicitly, the distribution of malicious software in general or the distribution of pornographic content. Furthermore, if (bulk) e-mails are directly addressed, many laws specify the type of e-mails covered, usually by focusing on commercial e-mails (UCE). For the purpose of litigation, legislators have to precisely specify when an e-mail can be regarded as unsolicited and when, thereby, its sender is violating the corresponding law. It should be noted that anti-spam laws avoid the usage of the term 'spam' because its legislative semantics have not yet been defined.

Sender and recipient

Laws can target specific types of senders and recipients to which they apply, such as private users and organizations. For example, the Directive 2002/58/EC (EU, 2002, Article 13.5) limits its 'generic' opt-in approach to recipients who are natural persons.

Possible accuser

Laws may impose a restriction on who can sue e-mailers. Many anti-spam laws, such as the United States CANSPAM Act 2003 (Public Law 108187, 16 December), do not provide legislative means for individuals, but only for state authorities and some other organizations such as ISPs (CANSPAM Act 2003, section 7). Likewise, the German *Gesetz gegen den unlauteren Wettbewerb* (UWG), section 8(3), opens the door to litigation for competitors, specific associations, chambers of commerce, chambers of crafts and some more 'qualified' organizations only.

Further requirements

Laws may make further requirements of e-mails. As mentioned above, the CANSPAM Act 2003, for example, prohibits the use of a harvested e-mail address, requires that advertisement or solicitations are identified clearly and conspicuously, and requires that each e-mail contains a functioning return e-mail address or other Internet-based mechanism that allows the recipient to opt-out of the commercial e-mail list. This list of further possible requirements of e-mails is far from being complete.

Anti-spam laws and international cooperation

Just as the volume of spam has increased since 2000, so too has the number of anti-spam laws around the world. Surveys carried out by the International Telecommunication Union (ITU) and the Organization for Economic Cooperation and Development (OECD) (both organizations sent out questionnaires mainly to their member states) found both a large number of anti-spam laws and a pronounced heterogeneity of the legislation (ITU, 2005b; OECD, 2005c). This heterogeneity is not surprising because of the high number of anti-spam law parameters in which the laws may vary (these were presented in the previous section). The studies presented detailed information about the anti-spam legislation in 47 countries. Country-specific information about 'consumer

protection agencies', 'data protection authorities' and 'communications regulators' with responsibility for the enforcement of laws related to spam are provided by the OECD (2005a) and ITU (2005b), with the latter also providing information about the international cooperation in which countries are participating. The Appendix summarizes which states have a designated (opt-in or opt-out) anti-spam law, which have any implicit anti-spam legislation, which have implemented the European Directive 2002/58/EC and when the laws were updated. (Portals containing links to legislative anti-spam laws can be found at www.spamlaws.com/ and http://notebook.ifas.ufl.edu/spam/Legislation.htm.) No legislation information is available for large parts of the world, such as Africa, the Middle East, large parts of Asia, and Latin America. We will now analyze legislation in terms of the parameters introduced above.

Subscription

When comparing worldwide legislation within those countries responsible for more than 50% of all e-mails classified as spam by many market research and anti-spam companies (Commtouch, 2006; Sophos, 2005; Spamhaus, 2006a, 2006b), we find that these countries (namely the United States, China, the Republic of Korea and Russia) either have a non-restrictive law such as an opt-out law, or have no anti-spam law at all. Countries with opt-in rules (i.e., most anti-spam laws contain opt-in rules; ITU, 2005b; OECD, 2005c), such as those that implemented the European Directive 2002/58/EC, were found to play only minor roles in sending spam. It is remarkable that most e-mails classified as spam still originate from the United States. This may be due to the fact that the CANSPAM Act 2003, which explicitly permits opt-out marketing, overrides state laws even if they are stronger (Allman, 2003).

Possible accuser

Legislation may impose a restriction on who can sue e-mailers. This restriction may, for example, exclude natural persons from any legal means by granting these means only to specific organizations such as national authorities or ISPs. In such a case, the prosecution of spammers can be channelized and controlled, but, contemporaneously, victims are excluded from direct influence on the prosecution process. As mentioned below, in the United States, the CANSPAM Act 2003, section 7, does not provide legislative means for individuals, only for state authorities and some other organizations such as ISPs. The EU provides a less restrictive regulation (EU, 2002, section 47): 'Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.' However, the German implementation of this EU requirement, for example, opens the door to litigation for some 'qualified' organizations only.

An example of a sophisticated regulation is the Australian Spam Act 2003 (www.comlaw.gov.au/comlaw/legislation), which differentiates as follows. Section 26 governs 'Civil action for recovery of pecuniary penalties': 'The ACMA [Australian Communications and Media Authority] may institute a proceeding in the Federal Court for the recovery on behalf of the Commonwealth of a pecuniary penalty referred to in section 24.' Section 28 governs 'Ancillary orders—

compensation': '[T]he Court may, on the application of the ACMA or the victim, make an order that the Court considers appropriate directing the perpetrator to compensate the victim.' And section 29 governs 'Ancillary orders—recovery of financial benefit': '[T]he Court may, on the application of the ACMA, make an order directing the person to pay to the Commonwealth an amount up to the amount of the financial benefit.'

Sender and recipient

The types of senders and recipients that legislation addresses determine its applicability to a large extent. Whereas the EU limits its approach to recipients who are natural persons (EU, 2002, Article 13 5.), the American legislation is less restrictive. The CANSPAM Act, section 3, includes both natural persons and organizations:

- 'The term 'recipient', when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered.'
- '[T]he term 'sender', when used with respect to a commercial electronic mail message, means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message. . . . If an entity operates through separate lines of business or divisions and holds itself out to the recipient throughout the message as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of business or the division shall be treated as the sender of such message for purposes of this Act.'

The Australian Spam Act 2003, section 7, explicitly includes both natural persons and organizations:

- '[T]he individual or organisation who sent the message, or authorised the sending of the message, is: (i) an individual who is physically present in Australia when the message is sent; or (ii) an organisation whose central management and control is in Australia when the message is sent.'
- '[T]he relevant electronic account-holder is: (i) an individual who is physically present in Australia when the message is accessed; or (ii) an organisation that carries on business or activities in Australia when the message is accessed.'

Scope

As indicated above, spam laws are either directed explicitly or implicitly against the sending of particular kinds of e-mails. As the 'Remarks' column in the Appendix shows, only 31 countries—the United Nations has 191 Member States, not including Vatican City (UN, 2005)—confirmed that they have explicit anti-spam legislation. Countries with such legislation mainly address commercial e-mails and UCE. The diversity by which laws can address the sending of (bulk) e-mails and related harm is illustrated by the following examples, with the first

three items representing implicit coverage and the last three representing explicit coverage:

- If a (spam) e-mail is fraudulent in some way, in the United States, this e-mail may be violating the Computer Fraud and Abuse Act, the Racketeer Influenced and Corrupt Organizations Act (RICO) and the Electronic Communications Privacy Act (ECPA) (Allman, 2003).
- The CANSPAM Act 2003, in principle, authorizes senders of commercial e-mails to send their UCE, unless the recipient has explicitly refused its receipt (section 1037): 'It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides (i) clear and conspicuous identification that the message is an advertisement or solicitation; (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender. (B) Subparagraph (A)(i) does not apply to the transmission of a commercial electronic mail message if the recipient has given prior affirmative consent to receipt of the message.'
- The European Directive 2002/58/EC (EU, 2002), which had to be implemented legislatively by each EU Member State by 31 October 2003, is aimed at protecting the rights of natural persons as well as the legitimate interests of legal persons. The Directive regulates some kind of opt-in mechanism and requires each direct marketing e-mail to contain information on how to cease the e-mail communication (EU, 2002, Article 13, section 1.4.): 'The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. . . . In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.'
- In Germany, the *Strafgesetzbuch (StGB)* (penal code) covers a broad range of delicts that may be committed if spam e-mails are sent. For example, it is a violation of the *StGB* to obtain computer resources surreptitiously (section 265a), modify data (section 303a), sabotage computers (section 303b) and disturb the proper working of telecommunication systems (section 317). The execution of malicious e-mail attachments such as viruses, worms and Trojan horses can lead to this kind of harm. Even the content of an e-mail can offend a law—for example, pornographic content (section 317) (BSI, 2005, pp. 48ff).
- In Germany, spamming can be regarded as an intrusion into a company's commercial activities according to *Bürgerliches Gesetzbuch (BGB)*, section 1004 (Köcher, 2004, p. 30).
- In Austria, the sending of e-mails to more than fifty recipients with the purpose of direct marketing violates *Telekommunikationsgesetz (TKG)*, section 107, unless the recipient has given acceptance prior to the sending.

Degree of the homogeneity of legislation

The ITU analyzed the zones of consensus and disagreement in existing legislation and found that laws strongly converge in the following instances

(ITU, 2005a, p. V): 'a focus on commercial content, the mandatory disclosure of sender/advertiser/routing, bans on fraudulent or misleading content, bans on automated collection or generation of recipient addresses, the permission to contact recipients where there is an existing relationship, the requirement to allow recipients to refuse future messages, and a mix of graduated civil and criminal liability.' The study also identified five key areas that are vital to a harmonized spam law, but have evaded consensus thus far (ITU, 2005a, p. V): 'a prior consent requirement for contacting recipients, a designated enforcer, label requirements for spam messages, the definition of spam (whether it is limited to e-mail communication, or includes other applications, such as SMS), and the jurisdictional reach of the system's spam laws.'

Summing up, there is no consensus on legislative attitude towards spam and its handling. There are still many countries that have no or low-effectiveness anti-spam laws and that, thereby, tolerate spammers, who have an incentive to locate operations in locations with less legislation and regulation. On the other hand, some countries have not only provided domestic legislation against spam, but taken action regarding international cooperation with other countries. These are partially open to private sector groups.

International cooperation

In the context of international cooperation, we can differentiate between bilateral government-to-government cooperation, private sector groups, government-to-private sector and multilateral cooperation (OECD, 2005b).

An example of an initially bilateral cooperation is the Memorandum of Understanding (MoU) between the United Kingdom and the United States, which was later extended to include Australia as well. The MoU provides a framework for cooperation in fighting cross-border spam affecting all three countries. Another MoU was signed by the Korea Information Security Agency, the Australian Communications Authority and the National Office for the Information Economy of Australia (ITU, 2003), which agreed upon closer cooperation and the exchange of information relating to spam in accordance with the relevant laws and regulations of each country.

Many more countries were involved in the multilateral 4Action Plan (London Action Plan, 2004). On 11 October 2004, government and public agencies from 27 countries responsible for enforcing laws concerning spam met in London to discuss international spam enforcement cooperation (member organizations come from Australia, Belgium, Canada, Chile, China, Denmark, Finland, Hungary, Ireland, Japan, Lithuania, Malaysia, Mexico, Republic of Korea, Spain, Sweden, Switzerland, the Netherlands, the United Kingdom and the United States). The purpose of the London Action Plan is to promote international spam enforcement cooperation and address spam-related problems such as online fraud and deception, phishing and dissemination of viruses. It is meant to be a simple, flexible document facilitating concrete steps to start working on international spam enforcement cooperation: 'The governments and public agencies intend to use their best efforts to encourage communication and coordination among the different Agencies that have spam enforcement authority within their country . . . , take part in periodic conference calls, at least quarterly, . . . encourage and support the involvement of less developed countries in spam enforcement' (London Action

Plan, 2004). In appreciation of public-private partnerships, the cooperation is partially open to the private sector, including ISPs, telecommunications companies, information security software providers, mobile operators, and domain name registrars and registries. It is intended that private organizations should participate in segments of periodic conference calls and assist in training sessions.

Other instances of multilateral cooperation include particular organizations that have been set up for anti-spam or other purposes. The OECD has created the OECD Spam Task Force, which arranges workshops and is currently developing an anti-spam toolkit—an instrument to help governments, regulators and industry players orient their policies relating to spam solutions. The ITU, the EU, the International Consumer Protection Enforcement Network (ICPEN) and the Asia-Pacific Economic Cooperation (APEC) are further examples of organizations that address spam multilaterally. For example, as well as the establishment of the European Directive 2002/58/EC and the proposal of a cooperation procedure concerning the transmission of complaint information (EU, 2004), the EU went a step further towards addressing spam by initiating the 'SpotSpam' project (EU, 2005). This project's aim is to facilitate legal action against spammers at the international level, and its core idea is that spam complaints can be submitted to the SpotSpam database via national 'Spamboxes'. The information stored in the database will enable appropriate authorities to take action against spammers. Additionally, law suits are more likely to be successful when they can be based on multiple end-user complaints in various countries.

An example of private sector cooperation is ASTA (Anti-Spam Technical Alliance), which was established by the Internet community and the companies AOL, British Telecom, Comcast, Earthlink, Microsoft and Yahoo!. ASTA recommends actions and policies for ISPs and ESPs and some other types of organizations including governments and online marketing companies. Although other forms of international cooperation have been set up (ITU, 2005a), this process is still at the fledgling stage.

Effectiveness

The implementation of laws addressing unsolicited bulk e-mail is believed to have had some minor or spotty effects on the spam plague at the most, although the press reports almost weekly on cases where e-mailers have been sentenced for spamming. Some cases brought under a specific anti-spam law and their status and outcome were reported by the OECD (2005a). However, apart from partial success stories, thus far anti-spam laws have not been able to stop the fact that about two out of three e-mails are classified as spam. The ITU (2005b, p. 9) points out: 'However, while the laws proposed to combat spam were put forth with good intentions they are not actually addressing the problem in a substantive way.' As previously mentioned, more than half of the spam e-mails originate from countries with no anti-spam law or with an opt-out rule. This indicates that opt-in laws have positive effects on spamming, whereas opt-out laws are ineffective. On the other hand, it must be conceded that opt-out laws are still useful because they repress the uncontrolled e-mail marketing of reputable companies. Consequently, a partially positive impact of anti-spam laws can be assumed.

A general problem of legislative measures against spam e-mails is that an international phenomenon is being addressed by national legislation. Going into detail, we find the following facts and problems:

- A substantial portion of received spam crosses international boundaries. An accompanying question for countries is whether they have jurisdiction over messages that originate within their borders, but are being sent to another country. Domestic provisions prohibiting the sending of spam, instituting rules for legitimate messages or requiring the labeling of messages are likely to have little effect on messages of extra-territorial origin (OECD, 2005b). Another question is whether a national authority or even a private user in a foreign country B is allowed to initiate litigation against a spammer who is residing in country A.
- The international legislative anti-spam landscape is heterogeneous and not transparent: even if a spammer violates a national anti-spam law of his or her country, and another country's entity is aware of this violation, the operational tasks involved in litigation (e.g., the involvement of national organizations) is likely to be difficult to perform. Moustakas et al. (2005, p. 7) stress this issue even more strongly: 'There can be no solution to the spam problem without some kind of worldwide ''minimum standard'' of legislation. Global harmonization is a very difficult task since the US and the EU have opt-out/opt-in regimes.'
- The litigation of a person or organization presumes that the sender has been identified. Two challenges arise in this context. First, the sender must be localized. If a sender uses address and name spoofing—and this is very likely to be the case—and also uses instruments for hiding, such as an e-mail proxy or third party hosts (e.g., bots), localization is difficult, if not impossible. And second, as with other forms of online crime, the regulation of spam and the enforcement of spam laws are complicated by difficulties associated with the collection and preservation of evidence (evidentiary burden) (OECD, 2005b).
- 'Several developing nations, such as India, have laws that prohibit hacking, stalking or harassment over the Internet, etc., but even then, the implementation of these laws is in the hands of the local police or other law enforcement organizations, who may be inadequately funded, ill equipped and poorly trained to keep abreast of cyber crime trends, let alone spam-related issues' (OECD, 2005c, p. 14).

It is especially the OECD and the ITU that have made suggestions on how to address these problems and therefore on how to improve worldwide anti-spam prosecution (ITU, 2005a; OECD, 2005b). First, the expansion of international cooperation is necessary to share information to further cross-border investigations and prosecutions involving spam. This issue includes the improvement of both the ability to cooperate and the cooperation itself with the relevant private sector entities. Second, law enforcement organizations should be funded, equipped and trained to be capable of investigating the often complex issues associated with spam and proceed to take action against offenders. Third, countries with non-restrictive laws or no anti-spam laws at all should switch to or introduce restrictive legislation so that the regions that spammers can move to without being endangered by legal prosecution are reduced or, even better, eliminated. In order to support a definition of anti-spam legislation that is both

effective and relatively equal in terms of levels of enforcement (the latter would support international cooperation), the OECD proposes constraints on the anti-spam policy and a checklist for the development of an anti-spam regulatory approach (OECD, 2005b). The ITU stresses that the harmonization of laws that regulate spam offers considerable benefits insofar as a model law could assist in establishing a framework for cross-border enforcement collaboration (ITU, 2005a). Although the ITU has not drafted a model law, it has framed and categorized the issues that drafters would need to take up. When supporting developing countries in introducing anti-spam legislation, one has to keep in mind that unlike many developed economies, developing countries often do not have the supporting institutions necessary to implement legislation effectively (OECD, 2005c).

Summary

Internet spam e-mails are not merely a cumbersome annoyance, but have even become a significant economic burden. Given this severity, the EU and the national authorities of many countries and federal states have started to address spam by legislation. However, today's worldwide legislative coverage of spam is heterogeneous and the existing laws differ in regard to several parameters, some of them being the kind of subscription (mainly opt-in versus opt-out), the law's scope, the type of sender and recipient addressed, and possible accusers. Just as the volume of spam has increased since 2000, so have the number of anti-spam laws and international cooperation efforts across the world. However, only 31 countries (the United Nations comprises 191 states in total) have an explicit anti-spam legislation, most of them containing opt-in rules. No legislation information is available for large parts of the world such as Africa, the Middle East, large parts of Asia, and Latin America. Thus far, anti-spam law could not stop the development of spam. More than half of the spam e-mails originate from countries with no anti-spam law or with an opt-out rule. This indicates that opt-in laws have a positive effect on spamming, whereas opt-out laws are scarcely prohibitive. On the other hand, it must be conceded that opt-out laws are still useful because they repress uncontrolled e-mail marketing of reputable companies.

A general problem of legislative measures against spam e-mails is that an international phenomenon is being addressed by national legislation. Today, the international legislation landscape suffers from obscurity regarding which country's jurisdiction can be applied when; heterogeneity and missing transparency; difficulty in identifying the sender; and insufficient funding, poor equipment and inadequate training of law enforcement organizations in developing nations. Key elements of an effective international anti-spam legislation are the introduction of (or switch to) domestic restrictive laws and the expansion of international cooperation. In order to support the development of a homogeneous (and effective) legislation landscape, it might be useful to provide a legislative blueprint for the implementing countries. The ITU, for example, has framed and categorized the issues that drafters of a model law would need to take up. However, considering the fact that two strong economic areas (the United States and the EU) have implemented very different types of legislation (opt-out versus. opt-in), it is doubtful whether legislative homogeneity will be achieved in the near future. Furthermore, the effectiveness of the American legislation has proven to be low, and it might be difficult to persuade this country to move to a more restrictive opt-in system.

References

Abadi, M. et al. (2003) Moderately Hard, Memory-Bound Functions. Paper presented at the Tenth Annual Network and Distributed System Security Symposium.

Allman, E. (2003) Spam, spam, spam, spam, spam: The FTC and spam, *ACM queue* (6)1, pp. 62–69.

Back, A. (2002) *Hashcash: A Denial of Service Counter-measure.* Available online at: http://www.hashcash.org/papers/hashcash.pdf (accessed 27 September 2006).

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2005) *Antispam—Strategien: Unerwünschte E-mails erkennen und abwehren* (Cologne, Bundesanzeiger Verlag).

Commtouch (2006) *February Virus and Spam Statistics: Swift Virus Attacks Continue to Gain the Upper Hand.* Available online at: http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=674&cat_id=1 (accessed 25 April 2006).

Dwork, C., Goldberg, A. & Naor, M. (2003) On memory-bound functions for fighting spam. In D. Boneh (ed.), *Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO 2003)* (Berlin, Heidelberg, New York, Springer).

Dwork, C. & Naor, M. (2002) Pricing via processing or combating junk mail. In D. Boneh (ed.), *Proceedings of the 22rd Annual International Cryptology Conference (CRYPTO 2002)* (Berlin, Heidelberg, New York, Springer).

European Union (EU) (2001) *Unsolicited Commercial Communications and Data Protection.* (Brussels, EU).

European Union (EU) (2002) 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) (Brussels, EU).

European Union (EU) (2004) Cooperation Procedure Concerning the Transmission of Complaint Information and Intelligence Relevant to the Enforcement of Article 13 of the Privacy and Electronic Communication Directive 2002/58/EC, or Any Other Applicable National Law Pertaining to the Use of Unsolicited Electronic Communications (Brussels, EU).

European Union (EU) (2005) *The European Spambox Project.* Available online at: www.spotspam.net (accessed 25 April 2006).

Fahlmann, S. (2002) Selling interrupt rights: A way to control unwanted e-mail and telephone calls, *IBM Systems Journal* 41(4), pp. 759–766.

Federal Trade Commission (FTC) (2004) *National Do Not Email Registry: A Report to Congress.* Technical report (Washington, DC, FTC).

Gabber, E. et al. (1998) Curbing Junk E-Mai via Secure Classification. Paper presented at the *Second International Conference on Financial Cryptography*.

Hall, R. (1996) Channels: Avoiding Unwanted Electronic Mail. Paper presented at the DIMACS Symposium on Network Threats.

Ioannidis, J. (2003) Fighting Spam by Encapsulating Policy in Email Addresses. Paper presented at the Tenth Annual Network and Distributed System Security Symposium.

International Telecommunications Union (ITU) (2005a) A Comparative Analysis of Spam Laws: The Quest for a Model Law. Background paper presented at the ITU WSIS Thematic Meeting on Cybersecurity, Geneva, Switzerland.

International Telecommunications Union (ITU) (2005b) *Survey on Anti-spam Legislation Worldwide.* (Geneva, ITU).

Köcher, J. (2004) Anti-Spam-Gesetze, *DFN Mitteilungen* 64(3), pp. 29–30.

Leibzon, W. (2005) *Email Security Anti-spoofing Protection with Path and Cryptographic Authentication Methods.* Available online at: www.metasignatures.org/path_and_cryptographic_authentication.htm (accessed 27 September 2006).

Loder, T., Alstyne, M. van & Walsh, R. (2004) *Information Asymmetry and Thwarting Spam.* Technical report (Ann Arbor, MI, University of Michigan).

London Action Plan (2004) *The London Action Plan on International Spam Enforcement Cooperation.* Available online at: www.londonactionplan.org (accessed 25 April 2006).

MessageLabs (2006) *Monthly Report: March.* Available online at: www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_de/intelligence_reports/march_2006/DA_153016.chp.html (accessed 25 April 2006).

Moustakas, E., Ranganathan, C. & Duquenoy, P. (2005) Combating Spam through Legislation: A Comparative Analysis of US and European Approaches. Paper presented at the Second Conference on Email and Anti-Spam (CEAS 2005).

Myers, J. (1999) *SMTP Service Extension for Authentication* (RFC 2554). Internet Engineering Task Force Network Working Group. (Sterling, VA, IETF).
Organisation for Economic Cooperation and Development (OECD) (2003) *Background Paper for the Workshop on Spam.* (Paris, OECD).
Organisation for Economic Cooperation and Development (OECD) (2005a) *Anti-Spam Law Enforcement Report.* (Paris, OECD).
Organisation for Economic Cooperation and Development (OECD) (2005b) *Anti-Spam Regulation.* (Paris, OECD).
Organisation for Economic Cooperation and Development (OECD) (2005c) *Spam Issues in Developing Countries.* (Paris, OECD).
Raz, U. (n.d.) *How do Spammers Harvest E-mail Addresses?.* Available online at: www.private.org.il/harvest.html (accessed 27 September 2006).
Sester, P. & Mutschler, S. (2006) Neue Kooperationen und rechtliche Entwicklungen im Kampf gegen Spam, *Informatik-Spektrum* (1)29, pp. 14–22.
Sophos (2005) *CAN-SPAM Act Can Do Better.* Available online at: www.sophos.com/pressoffice/news/articles/2005/12/canspam05.html (accessed 25 April 2006).
Spamhaus (2006a) *The Definition of Spam.* Available online at: www.spamhaus.org/definition.html (accessed 25 April 2006).
Spamhaus (2006b) *Statistics: The Top 10.* Available online at: www.spamhaus.org/rokso/index.lasso (accessed 25 April 2006).
Templeton, B. (n.d.) *E-stamps.* Available online at: www.templetons.com/brad/spam/estamps.html (accessed 27 September 2006).
Tompkins, T. & Handley, D. (2003) Giving e-mail back to the users: Using digital signatures to solve the spam problem, *FirstMonday* 8(9).
Turner, D. A. & Havey, D. M. (2004) Controlling Spam through Lightweight Currency. Paper presented at the 37th Annual Hawaii International Conference on System Sciences.
United Nations (UN) (2005) *List of Member States.* Available online at: www.un.org/Overview/unmember.html (accessed 25 April 2006).

Appendix

Country	Opt-in	Opt-out	Remarks	Year of last know law update
Argentina		x		2001
Armenia	No anti-spam law		Law on Personal Data deals with some aspects of spam.	
Australia	x			2004
Austria	x		*	2006
Belgium	x		*	2003
Brazil	No anti-spam law		Criminal, civil, anti-competition and pro-consumer laws exist, which could also be used against spam.	
Bulgaria	No anti-spam law		Some provisions of the Personal Data Protection Act deal with certain aspects of spam.	
Burkina Faso	No anti-spam law		There have been several draft laws proposed.	
Canada	No anti-spam law		Some statutes include some, although not all, of the measures generally available in spam-specific legislation.	
Chile		x		2004
China	No information available		The law prohibits the sending of e-mail with false or materially misleading information, the relaying of e-mails	2006

(*continued*)

Appendix (*Continued*)

Country	Opt-in	Opt-out	Remarks	Year of last know law update
			without authorization, the gathering of e-mail addresses illegally.	
Columbia		x	In 2004, the national legislature introduced a new bill that proposes an opt-out system. No further information is currently available.	2004
Costa Rica	Opt-in/opt-out system			2002
Cyprus	No information available		Section 6 of the Regulation of Electronic Communications and Postal Services Law 2004 (Law 12(I)/2004) deals with unsolicited communications (spam).	2004
Czech Republic	x			2004
Denmark	x		*	2004
Estonia	x		*	2004
Finland	x		*	2004
France	x		*	2004
Germany	x		*	2004
Hong Kong		x	The use of personal data for sending out e-mail spam for direct marketing purposes might be regulated by section 34 of the Personal Data (Privacy) Ordinance, which requires the sender to provide the recipient with an 'opt-out' choice of receiving no further marketing e-mails.	
Hungary	No information available		Article 14, Act CVIII of 2001 on Electronic Commerce provides for restrictions regarding unsolicited commercial communication.	2001
Ireland	x		*	2003
Italy	x		*Italy has enacted a tough anti-spam law that makes spamming a criminal offence punishable by up to three years' imprisonment.	2003
Japan		x		2005
Republic of Korea		x		2003
Latvia	x			No information available
Lithuania	x		*	2004
Luxembourg	No anti-spam law			
Malaysia	No anti-spam law		Act 588 provides that a person who initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his or her identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, thereby commits an offence.	

(*continued*)

Appendix (*Continued*)

Country	Opt-in	Opt-out	Remarks	Year of last know law update
Malta	x		*	2003
Mexico	No anti-spam law		The Office of the Federal Attorney for Consumer Protection reformed the Federal Law for Consumer Protection (FLCP) to add one chapter related, in general, to consumer protection in the context of electronic commerce. The amendments provide that 'suppliers shall respect consumer's choice not to receive commercial advertising'. These provisions could be interpreted in such a way to include spam under those articles.	
Netherlands	x		*	2004
New Zealand	x			2005
Norway	x			2003
Peru	x			2005
Poland	x		*	2002
Portugal	x		*	2004
Romania	x			2002
Russia	No anti-spam law			
Singapore	No anti-spam law		Legislative framework for the control of e-mail spam was proposed.	
Spain	x		*	2003
Sweden	x		*	2004
Switzerland	No anti-spam law		Anti-spam legislation will probably enter into force in 2007 and will be similar to EU law.	
Turkey	No anti-spam law			
United Kingdom	x		*	2003
United States		x	While many American states have also passed laws addressing spam, they are pre-empted by CAN-SPAM, except to the extent to which they address falsity or deception in commercial e-mail messages.	2004

Note: *In compliance with the European Directive 2002/58/EC.