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

15-Nov-2005

English - Or. English

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

DSTI/CP/ICCP/SPAM(2005)10/FINAL
Unclassified

Task Force on Spam

ANTI-SPAM REGULATION

JT00194053

English - Or. English

FORWORD

The OECD Task Force on Spam discussed this document at its meeting in October 2005, and recommended it for declassification to the CCP and ICCP Committess through a written procedure, which was completed on 11 November 2005.

This paper was prepared by Andrew Maurer, of the Australian Department of Communications, Information Technology and the Arts (DCITA). It is a contribution to the OECD Toolkit on Spam, and it is published under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

1. Introduction

Purpose of this document

The aim of this document is to aid the development and review of anti-spam regulation strategies and arrangements.

Restriction of scope – discussion not advocacy

It is recognised that the legal, political and cultural environments of different countries will vary, and that consequently there is no single uniform approach to spam that can be applied globally. Definitions of spam similarly vary between economies.

Accordingly, this document will describe the decision points that may arise in many jurisdictions, and discuss related policy questions rather than advocating a single approach. Any examples of existing regulatory regimes that may be referred to are intended to be illustrative of available options rather than a recommendation.

In referring to "spam" or "spammers" in this document the reference is intended to relate to material sent, or sent by persons, in contradiction of relevant national legislation or the prevailing societal norms.

Intended audience

This document is chiefly targeted towards jurisdictions:

- Considering the development of an anti-spam regime.
- Wishing to review existing regulatory arrangements.
- Looking to improve cross-border regulatory frameworks.

Structure of the document

This document briefly reviews the main characteristics of spam, and discusses the outcomes jurisdictions may aim for in formulating an anti-spam regulatory approach. A checklist of questions address the main decision points involved in formulating legislation, with subsequent sections of the document providing background for those questions.

2. Spam – what is it?

Introduction

The term "spam" is often used in the international media and in policy announcements made by different countries, however there is no commonly held definition of the term. Although broadly referring to the same phenomena, different countries define spam in a manner that is most relevant to their local environment. For this reason, in this document, the term spam refers to spam that is defined to be illegal. In any event, in developing an anti-spam policy, it is essential that the nature of spam be clearly understood and defined, and that spamming be differentiated from legitimate practice.

Countries wishing to develop anti-spam policy should identify which aspects of spam have relevance to their local political, cultural, legal and economic environment. In order to ensure an effective regulatory regime, they should endeavour to ensure that these aspects are capable of being objectively appraised through the consideration of physical and electronic evidence.

The common view of spam

The simplest view of spam is that it is any received message that is unwanted by the recipient. In terms of developing a policy response to spam, or anti-spam legislation, this definition is too broad and simplistic:

- It does not specify a messaging medium, and so could cover hardcopy letters, voice-to-voice communications, broadcasts as well as e-mail and other electronic messaging.

- There are a variety of legitimate messages that may be 'unwanted' by the recipient (invoices for purchased goods or services, credit card statements, for instance) despite the fact that they have agreed to receive them.

- A regulatory strategy needs to be such that senders of messages have an objective means of determining whether it is spam or not, before they send the message.

1. Despite these problems, it provides a starting point. Definitions will generally be the accretion of additional technical, economic, social and practical aspects of spam, described below.

Technical elements

Legislative definitions of spam may focus on a particular messaging medium, or attempt to provide a technology-neutral approach that provides an overarching statement of principles that is more broadly applicable. Even with a technology-neutral approach, it is worthwhile to evaluate which particular messaging media are being misused or causing problems within the jurisdiction, which media have a strong potential to be misused in the future, and which are unlikely to be misused within the jurisdiction.

The common options are:

- E-mail
- Instant Messaging
- Short Message Service (SMS)
- Other mobile spam and mobile messaging formats (such as multimedia messaging service, MMS)
- Facsimile

Although the most pressing problem for many countries is e-mail spam, countries with a strong take-up of third generation mobile telephony have found that SMS and MMS spam is of increasing concern. In some jurisdictions, concerns raised over spam have been raised in respect of telemarketing, Internet telephony (Voice over IP (VOIP)) and short range wireless communications (in the style of Bluetooth/wireless networking devices).

It should be recognised that any new policy or regulatory regime imposed on a messaging technology is going to have an impact on legitimate messaging, as well as the spam messages being targeted.

Commercial elements

The majority of spam is sent in order to achieve a profit – through the sale of goods or services, or through some sort of fraud. Arguably, one of the better ways of reducing spam is to reduce the economic benefits that the spammer receives from sending spam messages. For this reason, many legislative definitions of spam stress the commercial nature of spam – that spam is sent for marketing purposes or to achieve financial gain. If there are concerns that regulatory efforts against spam could have negative impacts on freedom of speech or expression, then a focus on commercial messages would clarify that political, religious or ideological messages would not be restricted by anti-spam activities.

Bulk

A common perception of spam is that it is sent or received in bulk. As the majority of e-mail traversing the Internet is indeed spam, its volume imposes costs in terms of bandwidth, supporting infrastructure, and the time that people spend dealing with unwanted messages. The volume of spam may reach such levels that it can operate as a denial of service attack, overloading servers and networks.

Spamhaus (www.spamhaus.org), an international anti-spam advocate, has estimated that more than 80% of the world's spam originates from 200 spam organisations. The US Direct Marketing Association similarly noted at the US FTC Workshop on spam that "While there are hundreds of thousands of … individuals who are causing the Spam problem, there is a huge volume coming from a relatively small group of folks or companies."

These messages are usually sent as part of a campaign – a large number of advertisements for a service or product are sent to thousands of millions of addresses. Spammers may send the messages from a single address, or use multiple different accounts and servers around the world to send spam. It is common for spammers to send their messages in a manner that disguises how many are being sent, and most often, who is actually responsible for sending them.

It should however be recognised that not all bulk messages are spam - there are many examples of messages that are sent in high volume entirely legitimately.

Misleading, pornographic or criminal content

There are obvious community and regulatory agency concerns with the illicit content of a considerable amount of spam - including those that promote pornography, illegal online gambling services, pyramid selling, get rich quick schemes or misleading and deceptive business practices. The stateless nature of e-mail has led to it being used to convey commercial offers and other content of a dubious nature, often with the true origin of the message disguised. The indiscriminate method of distribution is of particular concern as it is common for minors to receive spam that is pornographic, illegal or offensive.

In many countries this type of spam is already criminalised under existing laws or can be criminalized using the Council of Europe Convention on Cybercrime framework.

Vehicle for security threats

Spam may contain viruses and trojan software, often as a means of conveying yet more spam. As with other content-related issues associated with spam, the decision as to whether this should be addressed by the anti-spam regulatory regime is best decided with reference to the local circumstances. It should be recognised, however, that in many countries this malware aspect of spam is criminalised by statute or can be readily criminalised using the Council of Europe Convention on Cybercrime framework.

Ancillary elements

It is easy to consider spam as an activity only undertaken by the person who hits the "send" button. It can however be considered more broadly – often spam is sent on behalf of a third party, who hopes to sell goods or services to people responding to the messages. Increasingly, spam campaigns are being set up so that the person (or as mentioned, the trojan-controlled computer) sending the message is at several steps from the person that actually decided that the message should be sent. There is potential for a regulatory response to target the people who decide to send spam, or who collaborate in its sending, as well as the person physically responsible for sending it. There are a number of activities that serve to enable people to undertake spam campaigns. These include:

- The utilisation of software that harvests contact details and e-mail addresses from the Internet.
- The sale of address lists.
- The operation of "spammer friendly" ISPs.

It is important to note that there are beneficial and legitimate uses of address harvesting software (Webmasters could run the software against their own site, for instance, as a way of checking what contact addresses were being made publicly available). A regulatory strategy in respect of address harvesting, sale of lists or provision of a "safe harbour" ISP should only address these activities insofar as they relate to the sending of spam.

Can spam be legitimate messaging?

Legitimate messages are sent through the same messaging media as spam. Unless there is a desire to cease use of a messaging media, or prevent its use for commercial transactions, then any response to spam also needs to define what messaging is appropriate and lawful.

In developing a regulatory response, the choices are:

- To define classifications of messages based on technology, sender or content that will not be touched by the regulatory regime – that are outside of its coverage.
- To establish rules of practice that may be followed to be considered legitimate.

3. Identifying the goal of the anti-spam policy

Preservation of utility

Measures taken to prevent spam are designed to meet a number of policy goals and objectives; primarily they are concerned with preserving the effectiveness and efficiency of electronic communication. There is a delicate balance to be struck between businesses' ability to market their products and services and consumers' ability to be free from unsolicited messages. The level of spam, however, has now reached the point where it is impacting on users' confidence in using e-mail and other messaging media, and having a negative impact upon the performance of global communication networks.

Prohibition/punishment of spam

The implementation of anti-spam legislation and regulatory measures cannot be considered as the solution to the problem of spam; there is no 'silver bullet' to stop the sending of such messages, especially

due to the comparatively low cost of sending such messages. Legislation alone will not stop potential spammers from taking advantage of this marketing technique. Indeed, illegitimate spammers will likely ignore legislative provisions. However, laws regulating spam can serve the valuable public policy purpose of punishing those individuals and organisations that choose to make use of this methodology to harm consumers and therefore act as a deterrent to those individuals and organisations who are contemplating its use in this way. Having in place a framework that makes clear that such activities are in contravention of the law and that serious consequences may result from their breach, is an important tool in discouraging such behaviour.

Interdiction of spam

Anti-spam legislation in isolation may not necessarily result in a reduction of spam volume but it may provide a conceptual model and driver for the adoption and use of spam blocking software. Ensuring that ISPs are aware of spam's illegal nature may also operate as an incentive for such services to actively block spam on their communications systems.

Filtering of spam

One of the key concerns regarding spam is that it often contains inappropriate content – including pornography, illegal online gambling and unlawful trade practices. These concerns are amplified with the potential for such material to be received by minors.

Legislative provisions that encourage the labelling of e-mails as spam or prohibit the mailing of certain content may not necessarily result in an actual reduction in the volume of spam, but it may enable more effective filtering programs to operate and ISPs to actively filter such undesirable content This could enable users' to better identify spam and therefore control and prevent the influx of spam onto their computers. The labelling of e-mails may allow users to make more informed choices about the e-mails they receive. By its nature, filtering is a measure designed to govern legitimate messages; illegitimate actors will likely ignore labelling requirements, thus emphasising the need for strong civil and criminal enforcement authorities.

Reduction of spam

The key goal of anti-spam policy, and complementary legislative arrangements, is to reduce the level and severity of spam. Activities need to be targeted at a number of stages:

- Measures that are targeted to prevent spam being sent.
- Mechanisms to reduce the volume of spam traversing networks, after the spam has been sent.
- Reducing the number of spam received by end users - tools including filtering and interdiction (discussed above).

Conversion to legitimate practice

Anti-spam policies and legislative arrangements also serve to establish norms and best practices in relation to the use of messaging technology, and to encourage both individuals and organisations to act in compliance with such standards. The objective of such measures is to maximise the benefits of the use of such communications tools, whilst ensuring that the negative effects on networks and end users are minimised. An important aspect of the development of such codes of conduct and best practice is to ensure that they are well publicised. Such information should be readily available and accessible to the public,

industry and other interested parties. Governments should give consideration to the development of consumer awareness and education materials as an integral component of anti-spam policies.

Identifying measures of success

Given that it is unlikely that legislation/regulation alone will effect a reduction in the volume of spam, there are challenges involved in measuring the success or otherwise of such a framework. Problems are also encountered in the process of actually measuring the volume of spam and governments should give consideration to the development and use of appropriate metrics for its measurement.

Having a regulatory framework in place can impact upon the volume of spam being sent from within the jurisdiction, but this will be dependent upon having in place an effective enforcement regime. This should entail:

- A capacity to prevent the targeted behaviours/activities.
- A predictable, cost-effective process for the prosecution of offenders.
- Appropriate procedures for the handling of complaints.

Such a regulatory framework provides a stepping stone for international action - an important point, as most jurisdictions find spam crosses at least one international boundary in the path to a consumer's in-box. The existence of domestic legislation tends to aid effective international partnerships against spam, as jurisdictions that offer a safe haven for spamming activity are less likely to be invited to participate in reciprocal or collaborative action against spam than jurisdictions with effective anti-spam enforcement.

4. Identifying the constraints on the anti-spam policy

Origin of spam

A practical constraint for most countries developing an anti-spam policy is the knowledge that a substantial portion of received spam crosses international boundaries. Domestic provisions prohibiting the sending of spam, instituting rules for legitimate messages, or requiring labelling of messages are likely to have little effect on messages of extra-territorial origin.

Strategies that may mitigate this problem are:

- Initially, to ensure that domestic anti-spam measures are robust and effective.
- Seek partnerships and mutual agreements with other countries that have anti-spam measures in place.

Maintaining economic viability of the messaging medium

Most countries wish to stop spam, but not at the cost of stopping legitimate messaging. Decisions made in constructing an anti-spam regulatory approach may increase compliance costs or legal risks, particularly for businesses with a substantial online presence.

Strategies that may mitigate this problem are:

- Create a clearly defined model for legitimate electronic communications, preferably in consultation with industry sectors and public interest groups likely to be affected by a an anti-spam policy.

- Ensure that additional requirements imposed by an anti-spam regulatory approach are relatively easy to comply with.

- Ensure that any compliance requirements are clearly documented and are well publicised.

National jurisdiction and cross-jurisdictional issues

It is difficult to impose a regulatory approach on spam that crosses international boundaries. An accompanying question for countries is whether they have jurisdiction over messages that originate within their borders but are sent to a different country.

Strategies that may address this problem are:

- Institute civil and criminal extra-territorial statutes that specify messages sent to or from a jurisdiction, as well as messages commissioned from within a jurisdiction, are covered for civil and criminal enforcement purposes.

Hiding the origin of spam

A key challenge in the regulation of spamming activities, and the enforcement of spam laws, is the ability of spammers to obfuscate the origin of spam being sent. This can be done through a number of methods:

- *Spoofing of addresses* – spoofing is the term used to refer to the practice of forging e-mail headers so that the message appears to have originated from an entity or location other than the true source. This technique may be used by spammers to route spam through a reputable organisation as a means of enticing recipients to respond to their messages. This can have a negative impact upon the reputation of the victim organisation and can impose a significant cost burden on the organisation in repairing the damage done to it.

- *Open relays* – e-mail messages may be sent via a transfer agent that will deliver any mail for any sender, and fail to keep an accurate record of the sender's point of origin or the pathway that the e-mail has followed in reaching its destination. Spammers use open relays to avoid being traced.

These techniques increase the risk that prosecution of spam offences may be attempted against nearby or wealthy targets of opportunity, rather than the entity actually responsible for sending spam. This risk can be mitigated to an extent by ensuring that prosecuting bodies possess technical expertise, and by ensuring that physical and financial evidence can be admitted in the prosecution of a spammer.

Evidentiary burden

Like other forms of online crime, the regulation of spam and the enforcement of spam laws is complicated by difficulties associated with the collection and preservation of evidence. This is particularly the case where spam is travelling across international borders. It may be desirable for these concerns to be reflected in the development of legislation and in any consumer education material that may be prepared. Equally, the development of standardised approaches for gathering and providing electronic evidence, with a particular recognition of privacy issues involved in the cross-border transmission of evidence, may aid

the enforcement of not just the jurisdiction's spam legislation, but also of other laws pertaining to online crime.

It is particularly important that countries adopt uniform and consistent laws for the investigation and prosecution of cybercrimes, including criminal spam. This approach, which is reflected in the Council of Europe Convention on Cybercrime, greatly facilitates the sharing of information in cross-border criminal investigations and prosecutions.

It is also important to recognise that existing criminal law enforcement co-operation networks (such as the G8 24/7 Network) and mutual legal assistance instruments (such as mutual legal assistance treaties and letters of rogatory procedures) already allow countries to co-operate and share information in furtherance of criminal investigations and prosecutions involving criminal spam and other forms of cybercrime.

Timeliness of enforcement

If anti-spam laws are to operate as a true disincentive to spammers, then timeliness of enforcement of the laws is a critical issue. The conduct of court cases, especially where a right of appeal against an initial judgment is exercised, can take significant time. Enforcement agencies will generally need to act quickly in bringing the offender before the courts. Furthermore, as millions of spam messages can be sent daily, mechanisms need to be available so that action can be taken immediately to prevent the sending of spam, for example by recourse to injunctive relief. Non-government bodies such as ISPs may assist in responding rapidly to spam through the enforcement of Acceptable Use Policies (AUPs).

5. Checklist for the development of anti-spam regulatory approach: questions

Purpose of this section

This section of the report on *Anti-spam Regulation* presents the fundamental questions that need to be answered in order to design a regulatory approach that appropriately targets the anti-spam policy goals identified in the previous section. The considerations that should be taken into account in answering these questions will be dealt with in more detail in later sections of this document.

Nature of spam and objectives of the regulatory approach to spam

- Which spam attributes are of concern in your jurisdiction?
- Which are appropriately dealt with in terms of anti-spam policy or existing policy and regulation?
- What outcomes should be achieved by the anti-spam policy?
- What outcomes should be avoided by the anti-spam policy?
- Will the policy encompass the content of legitimate messages?

Technical elements

In terms of defining the scope of an anti-spam policy in relation to the coverage of **technical** issues, the following questions should be asked:

- What activities or artefacts will be covered by the anti-spam policy?

- Will the policy be based on a technology-by-technology description of covered messaging media, or will a more generic, technology neutral description be employed?

- If the policy deals with particular specified messaging technologies, how will it handle technological change?

- How would the emergence of a new messaging format be handled?

- How would the convergence of existing messaging media affect the policy?

- What if one of the technologies not currently covered by the policy becomes a spam problem - how would that be handled?

- If a "technology neutral" approach is taken, how much risk is there of the policy being applied too broadly?

- Will television, radio and other broadcasts be able to be excluded from the policy's coverage?

- Will Internet content be able to be excluded?

- How will voice communications be handled? How will voice communications that employ recorded messages or artificially generated voices be handled?

E-mail

- What commercial endeavours utilise or operate it? How will they be affected by a regulatory approach

- How do non-commercial organisations employ e-mail? Will a regulatory approach affect this use?

Instant messaging

- What size take up is there of instant messaging within the country? What is the projected take up?

- What commercial endeavours utilise it? How will they be affected by a regulatory approach?

- If e-mail is covered by anti-spam provisions and instant messaging is not, what potential is there for spammers to start employing instant messaging?

- If instant messaging is covered by the anti-spam regulatory approach, how will the enforcing body gather evidence? What records will be available and how can they be used?

SMS/MMS/ Mobile messaging

- What size take up is there of mobile phone messaging within the country? What is the projected take up?

- What commercial endeavours utilise it? How will they be affected by a regulatory approach?

- If e-mail is covered by anti-spam provisions and mobile phone messaging is not, what potential is there for spammers to start employing mobile phone messaging?

- If mobile phone messaging is covered by the anti-spam regulatory approach, how will the enforcing body gather evidence? What records will be available and how can they be used?

Convergence of messaging media

- Is it preferable to specifically target only those messaging technologies that pose a current spam problem, in the knowledge that if the situation changes the approach can be modified? Or

- Is it preferable to take the more difficult path of a general or technology neutral focus so that the regulatory approach can cover future changes in messaging without needing amendment?

Approaches to specific characteristics of spam

- Where bulk is characterised as an element of spam – how should 'bulk' be defined? How will standard spammer techniques of avoiding bulk provisions be dealt with?

- Can a single message be spam?

- How will the ability to send legitimate messages in bulk be preserved?

Messages with no recipient (dictionary attacks)

- When should a message sent to a non-existent address be considered spam?

Misleading, pornographic or criminal content

- Should the measures put in place to deal with spam also deal with issues relating to content?

- Would a broader focus compromise capacity to deal with spam in its own right?

- What capacity do existing laws have to deal with misleading, pornographic or criminal content? Are they sufficient?

Spam as a vehicle for security threats

- Do existing laws adequately deal with cybercrime and deliberate breaches of cybersecurity?

- Would a broader focus compromise capacity to deal with spam in its own right?

- How will the legal, cultural and economic environment of the local jurisdiction influence the design and operation of an anti-spam regulatory approach?

Ancillary elements of spam

- Should the regulatory response only focus on the person or organisation that sends spam, the entity that decides the spam should be sent, and the entity that benefits financially from spam? Or should all three of these parties be the target of regulatory responses against spam?

- Where legislation contains provisions relating to liability for the authoriser of the spam being sent, how will this authorisation be established? Will evidence of financial records and registered testimony meet the requirements relating to the acceptance of evidence?

- Where the origin/source of the spam is hidden or unavailable, how will identity be established? How is it determined who was involved?

- Should the regulatory response also cover activities ancillary to the sending of spam, such as address harvesting, sale of contact lists and provision of ISP services to spammers? How will the legitimate practices associated with these activities be protected?

- Who bears the burden of proof with respect to consent? How is such a requirement to be described and what actions may be taken to ensure the availability of the evidence?

- Where spamming activities breach rules relating to privacy and the handling of personal information, who bears the burden of proof with respect to compliance or otherwise?

- Which parties would appropriately have a role, or be affected by the regulatory approach?

- ISPs and carriage service providers can play a role in the regulation of spam. What legislative constraints will be in place upon them, such as privacy and interception laws?

- What would be the actual range of actions that ISPs would be expected to take? Court actions or just rigorous enforcement of terms and conditions? Would the blacklisting of known spammers from holding Internet accounts be included? Is legislation clear enough on the range of measures ISPs can take to stop or filter spam, and on how they can exchange information with public authorities?

- If ISPs undertook an enforcement role, what would their response be? There may be impacts in terms of cost, risk and technical overheads for the ISPs. Should there be a concern that this will reduce their competitiveness?

- Will the public react well to ISPs having this role? An element of public perception has been that some ISPs benefit from spam because they charge for bandwidth and downloads etc.

- Will ISPs be liable for the enforcement activities they undertake? There is a real potential for commercial loss and damage to reputation on the behalf of businesses targeted as spammers.

- In terms of the desired spam policy and regulatory approach, what are the appropriate actions available to the identified parties?

6. Checklist for the development of anti-spam regulatory approach: elements

- Defining spam's technological basis

Introduction

Spam is most commonly thought of in terms of e-mail. There are, however, a variety of messaging technologies that may be subject to the same problems as e-mail when it comes to spam. Technological developments and convergence may lead to the new messaging media arising or existing ones changing their form. In developing an anti-spam policy, the choice needs to be made as to whether a long-term approach is attempted, or a precise targeting of current problems is preferred.

Purpose of this chapter

This chapter outlines the main messaging technologies and issues particular to them. Additional information can be sought through resources such as www.wikipedia.org.

E-mail

Although different software packages are used to send e-mail and manage its transmission, the technical elements are well-known – it has a standardised format, and common protocols exist for creating, sending, receiving and reading e-mail.

Instant messaging

Instant messaging is a computer application that allows instant text communication between people over a network such as the Internet. In many ways, it is a simplified, more transient form of e-mail.

SMS/MMS/ Mobile messaging

Although the most pressing problem for many countries is e-mail spam, countries with a strong take-up of third generation mobile telephony have found that SMS and MMS spam is of increasing concern.

Bluetooth/wireless communication

Increasingly, personal electronics and mobile phones are being released with the ability to participate in wireless local area networks. Bluetooth is currently the best known industry standard for such wireless networks. The devices generally have an effective range of about 10 metres. There is the potential for such devices to be utilised in "proximity spam" – people walking past shops could have advertisements beamed to Bluetooth-capable mobile phones or personal data assistants (PDAs).

In considering the relevance of this scenario to a national anti-spam policy, the following could be evaluated:

- The take-up of local wireless devices.
- The likelihood of traders to undertake such proximity-based advertising.

Facsimile

Like e-mail, facsimile messages have a standardised format, and for a long time a common means of transmission – fax machines connected to phone lines scanned and printed out replicas of hardcopy documents. In many countries, facsimile spam predated e-mail spam, and caused a certain amount of ill-will – in terms of traditional fax machines, it was very clear that the recipient was being forced to pay for paper and toner to receive messages that they did not want. Due to this nuisance a number of "junk-fax" laws were enacted in the United States for instance – culminating in the Telephone Consumer Protection Act of 1991 (TCPA), a federal US law which provides that unsolicited advertisements may not be transmitted by telephone facsimile machines. Those using telephone facsimile machines or transmitting artificial or pre-recorded voice messages are subject to certain identification requirements. (See also www.junkbusters.com which contains information on potential legal action in the US against junk faxes: www.junkbusters.com/fax.html)

In recent years the boundary between facsimile messages and other forms of online communication have started to blur. Facsimiles are capable of being generated and read entirely on-line, with no hard copy

component. There is potential for optical character recognition software to further bridge the gap between the graphic format of facsimile transmissions and the text and graphic content of e-mails. It should be noted that excluding facsimile spam from restriction, while at the same time imposing restrictions on other messaging forms, could lead to an increase in the incidence of facsimile "spam".

Convergence of messaging media

The emergence of 3rd Generation (3G) mobile phone messaging has made e-mail and instant messaging available to mobile phone users. 3G and 4G telephony may further encourage the convergence of messaging formats. The increasing take up of Voice over IP (VOIP) may further accentuate convergence of messaging formats. In developing an anti-spam regulatory approach, it is useful to recognise that messaging formats will merge or evolve, and unforeseen messaging media may arise. In developing a regulatory approach, it is useful to consider both the local and international environment.

Clarity of definition

Vague definitions may mean that legislation has unintended coverage and application. In particular the developer of an anti-spam policy or regulatory approach should consider if terminology used may inadvertently cover:

- Radio/TV broadcasts.
- Ordinary voice telephony.

- **Consent**

A fundamental principle involved in many anti-spam regulatory arrangements is that e-mails of a commercial nature can only be sent to individuals or organisations where they have consented to receive such material. A number of conceptual frameworks have been utilised in relation to consent, including opt-in and opt-out models and provisions that allow for consent to be inferred where there is a pre-existing relationship.

One of the most fundamental issues surrounding spam legislation or regulation hinges around the issue of "consent" sometimes characterised as "opt-in versus opt-out" or on whether an activity is based on the permission of the recipient (ergo the term "permission-based marketing") prior to receiving the electronic message – 'opt-in' – or after receiving it – 'opt-out'. As well as being explicitly identified and legislated for, the concept of consent can also be incorporated through the application of personal and data privacy regimes, which may incorporate a presumption that unless consent has been given, then a person may not be approached or specific information (such as an e-mail address) traded or exchanged. The essential issue is the degree of consent or permission which legislators or regulators wish to require in specified circumstances.

Degrees of consent

Public debate about consent has tended to focus on the issue of 'opt-in' provisions versus 'opt-out'. While this debate was appropriate in the past, it is becoming less useful over time as many recent approaches to spam regulation have incorporated more complex or subtle approaches involving express consent, inferred consent, implied consent, assumed consent or a blend of these. These concepts are explored in more detail below, but it is important to remember that consent is often only one element of a spam definition or approach. Indeed, illegitimate marketers will likely not comply with either rule.

Express consent

This is the most straightforward form of consent where an individual or organisation has actively given their consent to a particular action or activity. Common examples of this include:

- A customer fills in a form, signs and provides personal details and permission to be sent future commercial communications.

- A voluntary check box or tick box appears on a form accompanied by an express statement that if the box is ticked by the recipient, the recipient may be sent commercial communications.

- A customer signs up for a trial or promotional offer where it is clearly stated that it is a condition of the offer that future commercial communications will be sent to them by the promotional provider.

- A person becomes a member of an organisation where the receipt of electronic messages from that organisation, or from sponsors and partners of that organisation, is expressly part of the membership agreement.

There are pros and cons in a regulatory system that exclusively relies on express consent (a strict 'opt in' regime). Express consent does provide a clear understanding between the message sender and recipient about the basis on which messages are being sent and their legitimacy. It can result in a much higher response rate for legitimate online marketers as the messages are from known or trusted senders, and therefore are much more likely to be read and relevant to the recipient. The reality for most businesses and consumers, however, is that their interactions tend to be on a less formal footing – a notification of consent may not be explicitly provided by the customer, or detailed records of received consent kept by business. The absence of such records may significantly restrict the potential pool of recipients who can be targeted for otherwise legitimate messaging, and the lists which can be purchased or used for this purpose. This in turn can reduce the number of persons responding and increase the costs of online direct marketing campaigns.

Some argue that the opt-in approach unfairly singles out legitimate marketers because illegitimate spammers will likely not comply. They also argue that an opt-in approach could lead to an enforcement approach that focuses on technical violations, rather than those violations that cause the most consumer harm.

In general anti-spam organisations and advocacy groups have advocated legislation based on express consent, arguing that consumers are entitled to a "right to be let alone" (see www.junkbusters.com/over.html). Direct Marketing organisations stated that such an approach may infringe "commercial free speech".

It should be noted that if anti-spam legislation relies on express consent, then the burden of proving that consent has been given lies with the sender of the message.

When challenged to provide evidence that a consumer has consented spammers have allegedly provided spreadsheets of random IP addresses from which the "consent" was allegedly received. To prevent this tactic it may be desirable to develop standards for record keeping of consent. One example of this is to utilise a 'double opt-in' process (sometimes also referred to as a 'closed-loop confirmation') which can be used to validate that an addressee has consented to receiving commercial electronic messages and provides supporting evidence.

The steps typically involved are:

A business receives a message saying that an electronic address (e-mail, SMS or similar) should be added to their contact list for commercial messages or company newsletters.

The business sends a message to that address, requesting confirmation that messages should be sent there in future. The message also contains a notification that the address will only be added to the contact list if a positive confirmation is sent within 14 days.

After 14 days, there are 3 choices:

- There has been a positive confirmation – the address is added to the contact list.
- There has been a negative response – the address is **not** added to the contact list for future messages.
- There has been no response – the address is **not** added to the contact list for future messages.

Requiring a "double opt-in" approach will generally remove any doubt regarding the validity of any claimed consent, but imposes further process on the business and consumer.

Inferred and implicit consent

This is consent which generally can be inferred from the conduct and/or other business relationships of the recipient. In terms of "business relationships" this could include a situation where the recipient has an existing and continuing association with the sender, for example as a customer, business associate, account holder, subscriber, member, licensee, registered user, employee, or contractor. The "relationships" aspect could be defined to extend beyond business relationships to include family and social relationships – it would rarely be desirable for legislation to impinge on communications between family members or friends.

Cases where consent can be inferred from "conduct" would generally reflect circumstances where the recipient has provided their electronic address without a clear statement that a particular person or organisation could use the address to contact them, but that nonetheless it would be reasonable for the address to be used in such a way. For example under the Australian *Spam Act 2003*, consent can be inferred where the recipient has chosen to "conspicuously publish" their electronic address in connection with their business or work-related function, (for example online or in a directory) they are taken to have consented to receive messages from any source that relate to that business or work function.

Assumed consent

"Opt out" legislation operates on the basis that there is a presumption of consent until it is removed by the recipient, for example by "unsubscribing" or by placing their electronic address on a do-not-contact-list, where legislation provides for that facility. This approach has generally been described as the "opt-out" approach. The US Can-Spam Act is an example of this approach.

Anti-spam advocacy groups generally oppose opt-out approaches for a range of reasons, including:

- It transfers the burden of effort and cost to the consumer.
- In order to unsubscribe the e-mail must be opened and responded to, which is contrary to good e-security practice, unless the e-mail is from a known and trusted source.

- Unsubscribe links are often non-functional.

- It places the evidentiary burden upon the recipient of the message.

On the other hand, some advocacy groups for e-marketers, such as the US DMA, advocate an 'opt out' approach because it is less constrictive to the operation of online commerce, and there is minimal risk of inadvertently proscribing legitimate messaging. In addition, companies that comply with opt-out laws have *functional* opt-out facilities, while usually spammers do not comply with any of the provisions foreseen by the legislation, either opt-in or opt-out. Further, they argue that this approach gives consumers who want to receive unsolicited offers a right to do so.

Blended approaches to consent

Some recent approaches to anti-spam legislation have provided a "blended" or situational approach to consent *i.e.* in some circumstances express consent will be required but in other circumstances it can be assumed or inferred.

More complex approaches to consent can increase the difficulty of drafting legislation, but can also assist in creating an approach which attracts the support of both anti-spam advocacy groups and direct marketing organisations. For example the Australian Spam Act attracted the support of the Australian Direct Marketing Association, as well as dedicated anti-spam groups such as the Australian Coalition Against Unsolicited Bulk E-mail, and Spamhaus.

Issues relating to consent

"Informed consent"

An issue that sometimes arises is whether, in providing consent, a recipient did so with a reasonable understanding of what they were consenting to, or indeed whether they were consenting to anything at all. Marketers have been known to operate on the assumption that in subscribing to something or ticking a box the user is agreeing to have their electronic address passed on to an indefinite number of other unnamed parties for other future solicitations. This raises the question of whether such consent is informed consent on the part of the recipient. To alleviate this uncertainty legislators may require that such a consent be highlighted, and not merely buried in the "terms and conditions" or restrict the degree of consent that can be granted, for example by:

- Restricting it to similar products or services as proved by the original provider.

- Placing a time-limit on the longevity of the consent.

- Requiring a confirming message which outlines the proposed usage of supplied information.

Removing consent or "Unsubscribing"

The ability of a recipient to remove consent, often through some form of "unsubscribe facility", is generally fundamental in spam legislation and should be incorporated in any legislation based on the principle of consent. There may be circumstances where, for specific classes of messages, there is no such provision. This may be done to avoid any infringement of issues of political or other free speech rights, or other policy considerations.

- **Privacy**

The regulation of spam may entail a significant overlap with privacy legislation and policies, and builds upon the idea that the use of personal data should be subject to acceptable (frequently legislatively-determined) norms. Thus, the sender of messages may be required to comply with such requirements.

However, it is worth noting that where such protection is available, it is only available to natural persons and not legal persons as privacy rights generally only attach to the former.

The term privacy in this context is generally linked to that of use of personal data. Depending on the jurisdiction, personal data may be considered to include information such as addresses (e-mail and otherwise), personal preferences and data such as age/medical conditions of individual natural persons. Unlike the concept of consent, personal data cannot be applied to legal persons such as corporate entities. The privacy principle assumes that the use of personal data (the sale, exchange, sharing of it) is subject to acceptable norms, which are usually concerned with and modified by personal choice.

Data Protection regimes aim to regulate the use and abuse of personal data. To the extent that e-mail addresses are personal data, then use, exchange or selling of these may be seen as illegitimate invasions on the privacy of the addressee.

Many countries, particularly in the EU, as well as EU-level rules (EU Directive 2002/58/EC on Privacy and Electronic Communications), have chosen to introduce anti-spam legislation within the framework of modifications of privacy and data protection laws. While the EU Directive, which sets down the principles of such modifications, leaves open the question of distinguishing between legal and natural persons within the scope of spam laws, a number of EU Member States have chosen to extend the logic of privacy and personal data into the definition of spam. Thus the United Kingdom, Ireland, France, Finland and Sweden apply anti-spam rules only to messages sent to natural persons.

- **Commercial elements**

The majority of spam is sent in order to achieve a profit – through the sale of goods of services, or through some sort of fraud. Arguably, one of the better ways of reducing spam is to reduce the economic benefits that the spammer receives from sending spam messages. For this reason, many legislative definitions of spam stress the commercial nature of spam – that spam is sent for marketing purposes or to achieve financial gain. If there are concerns that regulatory efforts against spam could have negative impacts on freedom of speech or expression, then a focus on commercial messages would clarify that personal, political, religious or ideological messages would not be restricted by anti-spam activities.

- **Bulk**

An option available to spam regulators is to specify a quantum of e-mails, whereby e-mails sent above this cut-off point are designated as spam and therefore blocked. This has generally been set at the level of 50 to 100 e-mails. However, such an approach is not without problems, as will be discussed below. One of the most significant problems with the bulk approach is its arbitrary nature; not all bulk e-mail is spam.

Not all bulk e-mail is spam. Bulk e-mail would probably not be generally regarded as spam if it:

- Is sent to recipients who have previously dealt voluntarily with the sender before and, on the basis of that existing relationship, can reasonably be assumed by the sender to be prepared to accept messages of the type being sent.

- Does not promote or include illegal content.

- Is not deceptive.

- Does not collect or use personal information inappropriately.

Common spammer techniques to avoid "bulk" provisions

Simple technical arrangements and legal arguments have been routinely employed in overseas jurisdictions to prevent messages from being classified as "bulk". The more common techniques are:

- Sending multiple flights of messages to multiple address lists of a size one less than the number defined as "bulk".

- Using multiple different addresses to send out the message.

- Using a simple program to insert random alphanumeric characters in each message sent to large address lists. It is argued that since no two messages are exactly the same, due to the inclusion of these random characters, they cannot be classified as a "bulk" message.

- Utilisation of anonymising and masking tools so that the recipient of the message cannot determine how many other recipients it has been directed to, or who they might be.

Problem with relying on 'bulk' as the exclusive definition of spam

A person who receives an unsolicited commercial message will generally not care, nor be able to discover, if the message has been sent to them singly, or to a million other recipients. Regardless of the number of other recipients, that person's time and resources have been consumed in dealing with the unwanted message, and their privacy has been invaded in a manner that should be addressed.

- **In breach of fair trade**

Spam legislation may be drafted to require that goods and services advertised and/or offered in messages must be legal, accurately described and commercially responsible. This may be useful in jurisdictions where the coverage of existing domestic consumer protection laws and laws relating to misleading and fraudulent conduct in respect of online or electronic messages is not clearly drawn out. A focus on whether the content of a message is misleading or fraudulent leaves aside many of the systemic concerns of spam.

- **Criminal or pornographic content**

A considerable amount of spam includes content of a dubious nature – pornography, illegal online gambling services, pyramid selling, get rich quick schemes or misleading and deceptive business practices. The indiscriminate method of distribution is of particular concern as it is common for minors to receive spam that is pornographic, illegal or offensive. Legislation may be drafted to particularly target criminal or pornographic messages, whether by making it part of the jurisdiction's definition of spam, associating additional penalties to messages containing these elements, or, in the case of pornography, requiring additional measures of compliance (such as labelling, described below). In many counties this type of spam is already criminalised or can be criminalised using the Council of Europe Convention on Cybercrime framework.

- **Damage**

Spam causes harm to a wide range of parties and systems. The costs to the victims of spam vary. From a systemic point of view, damage may be done by spam that effects a denial of service to parties, or by spam that is used as a vehicle for other malicious tools, for example, viruses. This systemic damage imposes costs in relation to infrastructure, human resources and in terms of opportunity cost when systems are damaged. Secondly, the cost of spam can be measured in terms of a focus on the content of the spam. Loss may be occasioned in this case through fraudulent or anti-competitive behaviour, such as phishing scams.

It is often difficult to quantify the damage caused by spam, particularly in instances where thousands of individual users receive spam from a single incident of illegal bulk e-mail. Legislative approaches to quantifying damages, particularly where a damage amount operates as a threshold to initiating a civil or criminal enforcement action, could include *i*) assigning a set monetary damage amount to each piece of spam sent or received (*e.g.*, Euro 1, GBP 1 or USD 1), *ii*) measuring damage based on the number of affected recipients (*e.g.,* an enforcement action could be initiated when at least 50 users within a jurisdiction are affected), or *iii*) measuring damage based on the number of spam messages received by a single entity, without a requirement to demonstrate an actual monetary damage amount (*e.g.*, an enforcement action could be initiated when a single user received more than 50 spam messages from the same entity within a defined time period).

- **Additional requirements – Legitimate messaging**

Labelling/Informed choice

Some legislation contains a requirement that spam e-mails be labelled. The labelling of e-mails as spam can be a useful tool in the fight against spam. If chosen, a requirement that messages be labelled would entail that the content of certain classes of messages (commercial, advertisements, pornographic) should be labelled, as per classification of films and publications – either as a prelude to state controlled censorship/regulation of access, or as method of informing the recipients' choice whether to open the message.

In terms of e-mail, labelling is the use of standard words in the message header or subject line that clearly identifies the content of the message, for example, the use of "ADV" for advertising and "ADLT" for adult content. Such a mechanism means that recipients are able to distinguish between advertising material and other e-mail traffic. It would also enable the more efficient and effective use of filtering systems, especially in relation to pornographic material, which may be sent to minors or in contravention of a country's laws.

Where e-mails are labelled as spam, the argument for labelling is that a user is better able to make an informed choice about whether to open e-mails or to filter them out. This is particularly critical given the increases in levels of spam that contain viruses and phishing scams. Labelling is potentially more problematic with non e-mail messaging technologies.

There are several limitations in relation to this approach, however. First, variations on labelling, may result in the evasion of filtering systems, for example, "A.D.V." or "a d v" instead of "ADV".

Second, there are two significant issues relating to the use of labelling which may present problems. Firstly, labelling would mostly be an effective anti-spam tool only if an internationally harmonised approach were adopted. This would be necessary to prevent problems emerging in relation to linguistic or alphabet differences between countries.

Third, spam offenders, especially those that obscure their identity and do not provide accurate contact details, are unlikely to comply with such a requirement.

- **Exemptions or restrictions**

The extent to which certain types of electronic messaging may be exempted from anti-spam regulation will depend on how spam is defined for the primary purpose of the regulation. For example:

- If spam is defined as "commercial" messaging, then exemptions may be appropriate for messages which have a commercial element but which are primarily non-commercial and which a government believes should not be prohibited.

- If spam is defined as "bulk" messaging, then exemptions may be appropriate for large-scale messaging which a government believes is in the public interest.

Scope of exemptions

A decision is required regarding which regulatory provisions can have exemptions. For example:

- Exemption from a general prohibition on sending "spam" may be useful to meet regulatory objectives (for example, Universities may enjoy an exemption from this prohibition in their communications with alumni).

- Exemption from a requirement for accurate contact and/or unsubscribe information may not be necessary to meet regulatory objectives (in the example before, while exempting universities can be useful to allow them to easily communicate with alumni, we do not need to allow them to send messages without accurate contact details or unsubscribe facilities).

Possible exemptions

Government Bodies: Messaging from government bodies may be appropriate to enable dissemination of information in the public interest.

Charities: Legitimate charities may reasonably wish to use electronic messaging for fund-raising and other purposes.

Political Parties: Messaging from political parties may be seen as a legitimate expression of free speech. This is obviously a sensitive issue which may vary between countries depending on national legal and political systems and cultures.

- **Additional elements – Spam**

Address harvesting

Address harvesting software collects people's contact details without their knowledge or permission. Address harvesting software and lists of contacts are fundamental tools in undertaking a spam campaign, and when used as an adjunct to sending messages are largely incompatible with express or inferred consent provisions in legislation.

There are, however, legitimate uses that address harvesting software and harvested lists may be put to, so a blanket prohibition is usually not desirable – a preferable middle course may be to levy additional

fines or penalties if such tools are used to aid the sending of spam in contravention of the jurisdiction's spam legislation.

Messages with no recipient (Dictionary attacks)

A common technique of spammers is to use 'dictionary attacks'. Rather than sending messages to an existing contact list, addresses are automatically generated based on words from a dictionary, common names and numbers. Messages are sent to the resulting addresses, without knowing whether they are valid addresses. The resulting flood of automated messaging imposes a substantial burden on the information and communications infrastructure, and can act as a "denial of service" attack on networks and online systems, despite the destination address being invalid. This imposes infrastructure costs, as e-mails, as messages using telephonic networks still use bandwidth and system resources in the transmission attempt.

7. Enforcement and sanctions options

Purpose of enforcement and sanctions

Enforcement regimes and legal sanctions have a number of uses:

- They ensure that compliance to defined legitimate messaging behaviours is mandatory rather than voluntary.

- They impose financial or other costs on spammers, lessening or removing the profits received from illicit activities, and therefore the motivation to undertake spamming activity.

- Their utilisation fulfils a normative role – providing directed feedback to society, or a segment thereof, that undesirable messaging behaviours will not be tolerated.

The timeliness and speed with which enforcement happens and penalties are applied is crucial, if spam is to be effectively curbed. Indeed spammers can move very fast and if needed, relocate their entire operations within days if not hours. Traditional enforcement notices which can take several weeks or months are no more effective in the online world.

Civil penalties

The majority of spam is sent with the intent of establishing a commercial relationship or otherwise gaining money. If it were clear that sending spam was not a profitable activity, fewer spam messages would be sent.

In considering the most appropriate structure for civil penalties, it is useful to bear in mind the overarching goal that penalties should, to the greatest extent possible, nullify the financial benefits to be obtained from spam and act as a disincentive for the sending of spam.

Countries may choose from a number of options available to them in imposing civil and financial sanctions upon spammers. Fines may be applied to those who breach anti-spam laws and regulations. These fines may be a flat amount per violation or vary in accordance with the nature and extent of the violation, for example, where there are repeat offences or offences in breach of an administrative order. Caution should be exercised in imposing a regime where a penalty is imposed for each and every breach as a single spammer may send millions of messages in a single day, thereby resulting in unfeasibly large penalties.

Another option available is to have provisions that require the recovery of profit obtained by the spammer. In such a case, this money can then be returned to the victims of the spamming activity.

The origin of spam is not often easily discerned. Where it is possible to determine the source, there may be further difficulties in identifying the individual/company who authorised the sending of the spam. This can create complexities in the imposition of penalties – penalties will only operate as a disincentive for the sending of spam if the originator of the spam is the party targeted.

Infringement notices

An infringement notice may detail one or many contraventions against a particular civil penalty provision that has occurred in one day. Separate infringements would generally be issued for contraventions against different sections, or for contraventions that occur on different days.

It may be useful to set a ceiling penalty amount that may be charged for all contraventions against a particular provision that have occurred in one day. Otherwise, an unrealistically large sum may fall due for multiple contraventions. There are reported cases of dedicated spammers sending millions of unsolicited commercial electronic messages each day.

Damages

Many jurisdictions provide natural or legal persons common law rights to seek compensation for damage received at the hands of another, with the compensation usually taking the form of financial redress. In the absence of a legislative construct, it may be difficult to demonstrate that spam has caused damage or substantial cost to the affected party, or to arrange that the spammer must make sufficient restitution that they would be discouraged from sending spam in the future.

Legislation could potentially be drafted to reflect the damage caused by spam, and to facilitate restitution of costs to damaged parties. Legislative approaches to quantifying damages caused by spam, particularly where damage amounts are relevant in the context of civil or criminal enforcement actions, could include:

i) Assigning a set monetary damage amount to each piece of spam sent or received *(e.g.*, EUR 1, GBP 1 or USD 1),

ii) Measuring damage based on the number of affected recipients (*e.g.*, an enforcement action could be initiated when at least 50 users within a jurisdiction are affected), or

iii) Measuring damage based on the number of spam messages received by a single entity (*e.g.*, an enforcement action could be initiated when a single user received more than 50 spam messages from the same entity within a defined time period).

Criminal penalties

Non-monetary sanctions, in the form of imprisonment may also be considered. This may be appropriate when the content of the spam breached criminal laws or where a spammer fails to comply with an administrative order. Criminal spam laws, such as the CAN SPAM ACT in the United States, may provide for significant punishments, including imprisonment, fines, and asset forfeiture.

It is important to recognise that criminal spam prosecutions form an important and necessary element of any spam enforcement regime. While civil enforcement mechanisms can adequately address many instances of illegal spam, there are some types of illegal spam (*e.g.*, transmission of child pornography and

facilitation of serious fraud) that can only be appropriately addressed through criminal prosecutions and criminal penalties.

Countries should be mindful, however, of the potential difficulties associated with such an approach. Higher evidential standards are applicable to such actions and criminal proceedings may result in a greater burden of time and resources, therefore resulting in a delayed result. Criminal penalties for spam will need to be consistent with, and reflect, the countries' approach to traditional criminal activity, for example assault and murder. There may also be reluctance on the part of the judiciary to impose criminal penalties in spam cases, especially where there is a lack of understanding of the impact of spamming activities.

Warrant - search and seizure

The evidence of illegal spam is generally electronic in nature and may be stored on many individual computers, devices, or networks in multiple countries or jurisdictions.

Therefore, enforcement authorities dealing with illegal spam need appropriate search and seizure authorities that include the ability to preserve, access, intercept, search and seize electronic evidence. Ideally, the focus of evidence gathering should be broader than just records of message transmission. Potentially financial records and related correspondence can help determine who commissioned the contravention, or was otherwise involved. Items that are found to have been, or are currently being, used to perform a contravention, or that would provide evidence of the contravention, could also be made subject to seizure. The Council of Europe Convention on Cybercrime provides a comprehensive procedural framework for cybercrime investigations, addressing such issues as the preservation, search and seizure of electronic evidence.

Given that spamming is something of a cottage industry, and can readily be done from people's homes, it would be wise to ensure that some checks and external oversight are placed on the investigating authority's ability to undertake search and seizure operations. In some jurisdictions, this would be handled through the issue of warrants.

Warrant - access to computer data

In many jurisdictions search warrants have traditionally been issued for a particular physical location or item. Electronic evidence presents unique issues in criminal investigations. The U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, has published a comprehensive guide to searching and seizing electronic evidence, located at: http://www.cybercrime.gov/s&smanual2002.pdf. The Council of Europe Convention on Cybercrime provides a comprehensive procedural framework for cybercrime investigations, addressing such issues as the preservation, search and seizure of electronic evidence.

Investigations – notification need not be given

In terms of the evidence that relates to spam offences, it is very easy for suspected spammers to arrange the loss, destruction or concealment of pertinent electronic records. If this is a concern, it may be useful to include delayed notice provisions for search warrants.

8. Identifying the involved parties

Spam is a complex issue, involving a large number of parties. Legislation needs to be designed to address the different rights and responsibilities of each player.

Individuals

Legislation should provide recourse to individuals harmed by spam. The rights of natural persons, as the recipients of spam, need to be protected by legislation and avenues for recourse need to be made available to them. Mechanisms need to be established to provide this, including avenues for the reporting of spam violations to an appropriate authority. Such complaints-handling procedures need to be transparent, efficient and effective.

Class actions

Where a large number of individuals are receiving spam, the potential exists for classes of individuals to join together and launch class actions against spammers. In such cases, challenges may be faced in terms of administrative issues, including the identification of individuals affected by a specific spam campaign, and the collection, retention and presentation of evidence. These issues, and the nature of spam being such that large numbers of parties may be sent spam, act against the likelihood of such a course of action.

Companies

Companies, like individual consumers, are also the recipients of spam. Legislation may thus be designed to provide avenues of recourse to them. Companies may be motivated to take action against spammers because of the commercial costs involved in dealing with spam and the distress caused to employees. This can create difficulties as their rights may not be equivalent to that of natural persons: for example, privacy rights do not necessarily extend to legal persons.

A second issue that emerges in relation to the application of anti-spam rules to companies is in relation to consent. Where there is a requirement that consent be obtained from a recipient before e-mail can legitimately be sent them, it is necessary to describe a mechanism whereby an authorised representative of a company can provide such consent on behalf of the company.

ISPs

ISPs have multiple roles in the arena of spam. They are the victims of spam, as spam can clog their networks and servers and thereby damage infrastructure. ISPs thus incur costs as a result of spam, in terms of damage to their hardware and also the costs and resources involved in dealing with spam. They are also both a source of spam and the intermediary through which spam passes. With regard to this latter role of ISPs, it is essential that an anti-spam legislative/regulatory framework does not impose upon ISPs a penalty for merely being the conduit by which spam is distributed. They are in effect, the mailmen of the and the delivery of messages should not equate to a responsibility for its content, nor damage caused by its sending.

ISPs are also potentially an important repository of evidentiary material that can be critical in the enforcement of anti-spam laws. However, the nature of this role should be clearly articulated: it may be necessary/desirable to describe the role of ISPs in legislative terms. This could allow ISPs, for example, to avoid breaching privacy roles where they are acting in support of government enforcement agencies. The use of Acceptable Use Policies (AUPs) by ISPs is another method by which the rights and responsibilities of ISPs can be described. An appropriately framed AUP can, in effect, allow ISPs to attain the status of self-nominated enforcer of anti-spam policies and are therefore a critical partner in the fight against spam.

Telecommunications providers

The principle that organisations should not be held responsible for spam where they are simply the intermediary through which spam passes is even clearer when applied to those service providers only

providing the telecommunications capacity or service (although many of the main telecommunications service providers are now also ISPs). For technical reasons the actual range of actions which telecommunications providers could be expected to take as regards prevention or limitation of spam is more limited than in the case of ISPs. Where actions may be imposed on such providers the same range of issues as noted above for ISPs apply.

Government agencies

Agencies involved in enforcement and monitoring of anti-spam regulation may include sector regulators (*e.g*. communications sector), consumer protection agencies and data protection agencies.

Law Enforcement agencies

Law enforcement agencies in many countries have authority to investigate criminal spam. It is important to recognize that spam may be implicated, either directly or indirectly, in many different criminal acts. Where spam involves broader crimes such as distribution or publication of illegal content, terrorism or threats to national security and critical infrastructure, then industry and regulatory agencies involved in anti-spam strategies and monitoring will need to co-operate with the appropriate police and government intelligence agencies.

Other interest groups

- Direct marketing associations.
- Consumer protection associations.
- Religious and political groups with a non-commercial interest in the sending of bulk messages.

9. Interaction with other domestic regulatory regimes

The regulation of spam interacts significantly with other, existing legislation in most countries particularly criminal statutes. These laws, even where not specific to spam, may apply to spamming activities, for example, laws to protect consumers from misleading or deceptive conduct or to regulate the distribution of pornographic material. Specific anti-spam laws, or the amendment of existing laws to apply to spam, need to be developed with a clear understanding of this potential for interaction and/or overlap.

Areas of legislative activity that may be relevant and necessary to take into account include:

- Privacy/data protection laws – for example, the European Union's privacy regulatory framework could be applied to many instances of spam.

- Cybercrime/security threats – spam is increasingly being used as a vehicle for the delivery of viruses, worms, spyware and other malicious tools and software. In most cases spam of this type is already criminal or can be criminalised using the framework in the Council of Europe Convention on Cybercrime.

- Misleading/fraudulent/deceptive content – Spam is increasingly being used as a vehicle for fraud, for example, phishing scams. Such activities may be covered under existing anti-fraud laws, consumer protection legislation and/or pornography laws.

An example of a domestic survey of existing laws and their applicability to spam is available at: www.dcita.gov.au/ie/publications/2003/04/spam_report/matrix.

10. International and cross-jurisdictional issues

Like many activities conducted via the which governments may seek to regulate to protect consumers and minors – for example, gambling and offensive content – spam presents problems of enforcement of national laws. Spammers who are apparently breaching the laws of a particular country may well be located in a variety of geographic and technical locations.

Extra-territorial jurisdiction - that is the legal authority of a government to exercise authority beyond its normal boundaries – is a potentially complex legal issue which may, as a matter of general legal policy, vary from country to country. However, it is increasingly common for countries to assert some form of extra-territorial jurisdiction in important legislation when appropriate.

For the purposes of preparing and implementing anti-spam regulation, the issues to consider are:

- Incorporating measures that can practically be enforced by national courts.
- Providing for any relevant international agreements.
- Cross-border enforcement at the operational level.

Enforcement by national courts

Enforcement of anti-spam regulation against "international" spammers may be more workable if the regulation creates a link with domestic corporations and persons, for example:

- Spam is being sent from the country in some way, including use of servers or other technical platforms on a "relay" or "third party" basis.

- Spam is being sent to domestic corporations or persons in some way.

Relevant International Agreements

There are currently no multilateral agreements of a binding nature which deal specifically with the problem of spam.

It may be prudent to include in anti-spam regulation the ability to implement any such agreements or conventions should the national government decide to enter into one or more. This would ultimately be a choice for national government.

Existing criminal law enforcement co-operation networks (such as the G8 24/7 Network) and mutual legal assistance instruments (such as mutual legal assistance treaties and letters rogatory procedures) already allow countries to co-operate and share information in furtherance of criminal investigations and prosecutions involving criminal spam and other forms of cybercrime. Civil enforcement authorities should keep in mind existing law enforcement co-operation networks and mutual legal assistance instruments as they evaluate the need for non-criminal spam enforcement co-operation mechanisms.

Cross-border enforcement

In the absence of formal multilateral civil enforcement agreements, there is growing co-operation at the operational level between a wide range of anti-spam regulators around the world. Several anti-spam regulators have agreed on a broad co-operative framework, the "London Action Plan". Information on the London Action Plan is available at: e-com.ic.gc.ca/epic//inecic-

ceac.nsf/vwapj/London%20Action%20Plan.pdf/$file/London%20Action%20Plan.pdf and some countries have entered into bilateral agreements on anti-spam activities.

In general, the evidentiary challenges associated with enforcing spam legislation can become more marked when the spamming activities cross borders and co-operation between national agencies is required for prosecution. If national anti-spam regulation explicitly supports regulators to assist their counterparts in other countries in gathering evidence as part of investigating possible offences, the efficacy of co-operative arrangements will be greatly enhanced. More generally, cooperation is enhanced where national legislation is broadly consistent between countries as advocated in the Council of Europe Convention on Cybercrime.

11. Adjunct activities – codes of conduct/codes of practice

While it is clear that legislation is a key tool in the reduction of spam, legislation alone will not solve the problem. One component of a multilayered approach to spam is the development and use of codes of conduct and codes of practice that reflect best practice in sending legitimate messages or dealing with spam messages.

Work has already been undertaken by a range of parties to implement self-regulatory approaches to reducing spam. Activities in this area include those generated by anti-spam organisations, Service Providers, the industry, marketing companies, consumer advocacy groups and end-users.

Industry bodies can put in place codes of practice and guidelines that support and encourage compliance with legislative/regulatory arrangements and, where possible, bring industry in line with best practice.

Examples of issues which such codes might address include:

- ISPs providing customers with information about the use, availability and appropriate application of filtering software.

- The e-marketing industry may undertake activities to ensure that spam sent to minors complies with responsible and ethical practice.

- Procedures for ensuring that consent to receive such messages has been validly received, and that a withdrawal of such consent is acted upon appropriately and within reasonable time frames.

Industry **standards** may also be another useful mechanism by which compliance with anti-spam laws is maximized. They can reinforce industry codes and may also be developed where industry has not put in place codes of conduct, or where compliance with such codes is problematic.

While there is significant value in the development and use of codes of conduct, codes of practice and other documents providing for best practice, it should be borne in mind that such mechanisms have limitations as to their usefulness. Few spammers are members of the relevant industry bodies and are unlikely to be inclined to act in accordance with such voluntary schemes.

The UK Direct Marketing Association has developed a code of practice for e-mail marketing: www.dma.org.uk/content/Pro-BestPractice.asp

The London Exchange has developed a Best Current Practice intended for ISPs with the aim of combating unsolicited bulk e-mail: www.linx.net/noncore/bcp/ube-bcp-v2_0.html.

12. Implementation

Protecting legitimate business

One of the principal goals of an anti-spam regulatory framework is ensuring that the negative impact of such a regime on business is kept to a minimum. It should be made clear that compliance with anti-spam measures can result in positive outcomes for individuals and businesses; by complying with the requirements of the legislation, there is an increased opportunity for legitimate and appropriate advertising/marketing material to be received by the intended audience.

It is critical that resources are made available to provide consumer awareness and education materials to users, especially business. This will ensure that there is an understanding of the goals of anti-spam measures and the way in which they can operate to enhance business activities.

A number of steps can be taken to maximise compliance by business with anti-spam laws:

- Provision of grace periods before the legislation comes into effect. This provides affected businesses and individuals with an appropriate opportunity to examine their current practices and modify them, as required, to reflect the requirements in the legislation.

- "Grandfathering" provisions provide business and individuals with the opportunity to contact their existing address lists and seek the consent of them to continue to receive e-mails.

Quantitative and evidentiary considerations

A key challenge in the effort to prevent spam is in understanding the true scope of spam and its impact. Further detailed data is required in the following areas:

- The nature and extent of the problems caused by spam.

- The rate of growth of spam.

- The success of the various proposed solutions to spam.

Such data would better inform the development of anti-spam policies, both nationally and internationally, and would provide countries with a means of measuring the success of anti-spam initiatives.

The lack of reliable and detailed information and data with respect to spam has a clear relationship with the issues pertaining to the evidence that might be available to ensure appropriate and effective enforcement of spam laws.

The investigation and prosecution of spam cases can be complicated by the following practical issues:

- Locating the true originators of spam.
- Establishing jurisdiction.
- Enforcement of remedies, especially where inter-jurisdictional.

Even where such issues are straightforward, the obtaining, preservation and presentation of the evidence relating to these and other issues, may be problematic.

Behaviour modification

The purpose of anti-spam regulation will generally be to prevent or minimise spamming behaviour by individuals and corporations. That is, the "success" of regulation should be measured in terms of actual changes in behaviour rather than, for example, successful court cases. This can be achieved by providing for:

- Powers for the regulator to issue warnings and accept undertakings instead of immediate court proceedings.

- Incentives other than legal sanctions to reduce or stop spamming behaviour.

Warnings

The regulator could be empowered to issue a formal warning rather than initiate full court proceedings. This would give some flexibility where the behaviour is largely inadvertent and unlikely to be repeated, for example in the early stages of anti-spam regulation coming into force when not everyone is aware of its requirements.

Issuing a warning should not necessarily prevent subsequent court action.

Undertakings

The regulator could also be empowered to accept formal administrative undertakings from individuals or corporations as an alternative to immediate court proceedings. These undertakings could be made enforceable by the courts if they are breached.

For example, the regulator may accept an undertaking from a person that they will not send any further spam (however defined), that they will implement or amend an unsubscribe facility or that they will verify their contact address database to eliminate addresses that may have been included from past harvesting activities.

Accepting an undertaking should not necessarily prevent subsequent court action if the undertaking is breached.

Incentives

The most significant incentives for spammers to modify their behaviour in the long term may well be commercial and technical, which are difficult factors to address through regulation alone.

Regulation can encourage responsible behaviour by parties such as direct marketers and Service Providers by recognising industry codes of practice and standards as a way of achieving the objectives of the anti-spam regulation. If compliance with such codes and standards is seen as responsible corporate behaviour by industry, then the incidence of spamming should reduce at least at the national level.

Public information and awareness

Implementation of anti-spam regulation will be most effective if the regulatory arrangements are fully explained to:

- Businesses which may be **sending** legitimate electronic messaging and who do not wish to inadvertently breach any anti-spam regulation.

- Businesses which may be **receiving** spam and wish to complain.

- Consumers who may receive spam and wish to complain.

Different communications strategies, including publications, may be appropriate for each of these groups. In particular, local business, direct marketing and consumer bodies would normally have an incentive to work with regulators in implementing anti-spam regulation. Information on these groups can be found at:

- Direct marketing associations: http://www.the-dma.org/affiliates/dmintl.shtml.

- Consumer bodies: http://www.consumersinternational.org/about_CI/GlobalMap.asp?regionid=135.

Examples of educational material on national anti-spam regulation can be found at:

USA: http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.pdf

Australia: http://www.dcita.gov.au/__data/assets/pdf_file/21725/DCITA-Spam-4Bus-Web.pdf

UK: http://www.oft.gov.uk/Consumer/Spam/default.htm

APPENDIX A - SYNOPSIS OF ANTI-SPAM STRATEGIES

Appendix A aims to provide brief and general summaries of the key elements in existing anti-spam laws in a number of jurisdictions. The descriptions in this section are not intended to be comprehensive, but rather to identify the most important ingredients of the laws in such a way as to be comparable and useful for other jurisdictions that are developing their own legislation in this area.

1. Australia

The Australian *Spam Act 2003* is consent-based legislation that covers commercial electronic messages, including e-mail, instant messaging SMS and mobile messaging. The term "commercial" is taken to include offers to buy or sell goods, service or land, to provide investment or other financial opportunity. Commercial electronic messages may only be sent with the express or reasonably inferred consent of the addressee, must contain clear and accurate identification of the sender, and must include a means of opting out from future messages. Address harvesting and address harvested lists may not be used in the course of sending commercial electronic messages. "Dictionary attacks", which involve sending commercial electronic messages to non-existent addresses, are not permitted.

Enforcement is undertaken by the Australian Communications and Media Authority (ACMA), which has the power to send formal warnings, issue fines and undertake court actions in respect of breaches of the Act. Courts may impose financial penalties for breach of the Spam Act, issue injunctions against further spamming activity and may additionally require spammers to surrender any financial gains from their spamming activity. There is no private right of action under the provisions of the Act, although persons suffering damages may seek compensation for a breach of the Act that has been the subject of a court determination.

The Act does not supersede individuals' right to undertake a common law action for damages.

2. EU Directive countries

EU Directive 2002/58/EC on Privacy and Electronic Communications is consent-based legislation applying to messages for the purposes of direct marketing via e-mail or other electronic messaging systems (SMS, MMS). It requires that prior consent of the recipient must be obtained before unsolicited commercial e-mail be sent to any natural person, unless contact details were obtained within the context of an existing customer relationship. Member states may chose to extend the requirements to legal persons.

All direct marketing messages must clearly and accurately identify the sender, which includes a valid address to which recipients can send a request to stop such messages. Address harvesting is prohibited under provisions of the general Data Protection Directive 95/46/EC.

Enforcement of EU Directives lies with the Member States. However the Directive requires that infringement penalties and remedies must be in place and that individual rights to judicial remedy and compensation for damages must be provided.

3. United States

The US Can-Spam Act ("Controlling the assault of Non-Solicited Pornography and Marketing Act" – 117 Stat. 2699 Public Law 108 – 187, Dec. 16 2003) applies to e-mail whose primary purpose is advertising or promotion of a commercial product or service. The CAN SPAM Act prohibits deceptive subject lines, failure to provide an opt out method and honor opt out requests, failure to include a valid physical postal address and, for sexually-explicit messages, failure to include a warning label.

Automatic address "harvesting" and "dictionary attacks" are not independent violations, but they trigger increased penalties.

Enforcement of the act is primarily the responsibility of the Federal Trade Commission (FTC), as well as the Department of Justice (DoJ) as regards its criminal sanctions. The FTC has the power to issue financial sanctions for non-compliance with the Act. Although civil and regulatory provisions are the primary mechanism by which the Act is to be enforced, the Act also created several new federal crimes in Title 18 United States Code, Section 1037. These new crimes are intended to address more egregious violations of the Act, particularly where the perpetrator has taken significant steps to hide his or her identity from recipients, service providers, or investigators. These crimes are punishable by imprisonment, fines, and asset forfeiture.

4. Korea

The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. prohibits the transmission of spam. Spam is defined as the sending of an electronic commercial advertisement against the addressee's explicit rejection of such information. The definition of spamming media was expanded in December of 2002 to include telephone, fax and other electronic multi-media.

The approaches are blended into the Act, which can require an expressed consent for sending an electronic commercial advertisement to wired/mobile phones or fax, while applying opt-out (assumed consent) for e-mail messages in general.

The Act includes strict labelling requirements for legitimate advertising messages. The sender is required to expressly indicate the objective of transmission and major contents thereof. "ADV" (for advertisement) or "ADLT" (for adult content) must be included in headers wherever relevant. Transmission of adult content advertising to minors is prohibited.

The name and means of contacting the sender must be included in all advertising messages, as well as clear instructions for opting-out of future messaging. An opt-out request may not be disregarded or avoided through technical manipulation.

The collection of email addresses by using a program or other technical means is prohibited, as is the act of sharing, selling or exchanging lists of e-mail addresses harvested from Internet bulletin boards or automatically generated (so-called "dictionary attacks").

5. Japan

In July 2002 two laws regulating spam came into effect. One is the Law on Regulation of Transmission of Specified Electronic Mail (Law No. 26, 2002). The other is an amendment updating the 1976 Specified Commercial Transactions Law (Law No. 28, 2002). The new rules prohibit unsolicited commercial e-mail messages being sent to anyone who has expressed a wish not to receive such messages. They include labelling obligations on all advertising messages: direct marketers must specify in each

unsolicited commercial e-mail message that it is an advertisement and that it has been sent without permission. This way users have the option to automatically block all mail that contains unsolicited advertising. Alongside this direct marketers must provide a valid return address and subject line in each message, as well as the means of opting out of future messages.

Sending of direct marketing mail to randomly generated e-mail addresses is forbidden.

Government issues administrative orders to make illegal senders or comply with the law. Senders that violate the order can be subject to substantial penalties.

APPENDIX B - MATRIX OF ANTI-SPAM LAWS

Appendix B provides, in draft version, a matrix comparing the key elements of existing national anti-spam laws in 19 OECD countries. The blocked areas in the vertical columns under each country (listed across the top row) identify which of the regulatory elements (listed in the left hand column) are included in that country's anti-spam laws. The objective is to provide a graphic road-map of building blocks for anti-spam rules for countries wishing to use and learn from existing rules around the world to develop their own legislation.

At this stage, the blocked areas indicate only those areas where information has been found. Thus, the non-blocked spaces do not necessarily represent areas where rules are absent, but rather, those areas where rules have not yet been identified by research to date.

On the scope of spam, as mentioned in Appendix A, the EU Directive 2002/58 refers specifically to 'commercial e-mail' and 'for the purposes of direct marketing'.

	AU	AT	BE	CA	CH	DE	DK	ES	FI	FR	GB	IE	IT	JP	KR	NL	PT	SE	US
Defining scope of spam																			
Commercial nature	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■
Messaging Tech defined	■	■				■	■		■		■	■	■		■	■	■		
Bulk		■																	
General consent requirements																			
Express	■	■	■	■		■	■	■	■	■	■	■	■			■	■	■	
Inferred	■							■						■		■		■	
Assumed					■									■	■				■
Distinctions regarding consent requirement																			
Different provisions for legal vs natural persons									■	■	■	■						■	
Identity and transparency requirements for legitimate message																			
Sender I.D.	■	■	■		■		■	■	■	■	■		■	■	■				■
Valid return address	■	■	■		■		■			■	■		■	■	■			■	■
Unsubscribe	■	■	■		■		■	■	■	■	■	■	■	■	■		■	■	■
Information in headers and message														■					■
Labelling								■	■		■			■	■				■
Address abuse																			
Harvesting	■							■							■				■
Dictionary attack														■					■
Disclosure / sale of personal data				■				■		■	■	■	■		■				
Penalties																			
Financial	■	■						■			■		■	■	■			■	■
Criminal								■					■	■					■
Damages	■							■											■
Surrender of profits	■							■											
Industry codes	■							■					■	■					