



MessageLabs' response

**Hong Kong Consultation Paper
on the Proposal
to contain the problem of
Unsolicited Electronic Messages.**

Submitted: 25 October 2004

Executive Summary

MessageLabs welcomes the opportunity to respond to this Hong Kong consultation paper. This response provides a technology vendor's perspective on the spam problem on a global scale and on how to tackle spam – the way ahead.

MessageLabs is a leading global provider of internet security solutions and has maintained its Asia-Pacific base of operations in Hong Kong for the past four years.

To put the legislative process into perspective, MessageLabs has turned to what other countries around the world are doing to combat spam to provide examples and a framework for this response.

Currently, in the Asia-Pacific region, Australia, Korea and Japan have adopted some form of anti-spam legislation. The Australian legislation has been critically acclaimed as the strongest globally.

Outside of Asia Pacific, the EU spam legislation was enacted in December 2003 and is open to interpretation (legal and otherwise). However, not all EU countries have yet adopted it (although they are legally obliged to do so), the implementation is patchy, and areas of cross-border jurisdiction are not yet clearly defined.

The US spam legislation was enacted in January 2004 – the CAN SPAM Act. It was designed to regulate an otherwise unregulated industry and intended to prevent fraudulent and misleading spam sent illegally.

MessageLabs believes that legislation alone is unlikely to ease the spam epidemic. A legal framework is only part of an overall solution and requires international cooperation and enforcement.

The primary advantage of properly considered and enforced legislation is that it will make spamming less appealing, more difficult to operate and therefore less profitable.

The majority of recent legal actions in US exercised existing legislation to combat fraudulent or deceptive practices, rather than the CAN-SPAM Act. A balance between “Locks” vs. “Laws” is required, yet current legislation is only a starting point: there is the question of ‘opt-out vs. opt-in’ and there is the additional problem that most spam is now “dressed-up” to appear legitimate under opt-out laws.

Even with the introduction of legislation, spam will not simply go away, and each of these recent measures will need time to settle as they are implemented and proven over time. It is possible to manage an anti-spam solution internally for the short-term, but this requires that the administrator of that system to be able to respond quickly and accurately to new spammer tricks and techniques.

Gradually, users may notice a decline in spam reaching their inboxes, but huge volumes are still being delivered to the email gateway in order to be filtered. These bandwidth costs, and the impact of running email servers at increasingly high tolerance thresholds are only likely to increase problems in the fullness of time.

Spammers are already finding new ways to circumvent the statistical filtering methods, and as we have already seen, they are becoming more sophisticated. As this level of sophistication improves, the only way to combat the problem will be to employ a combined approach to combating spam.

In addition to legislation around the world, technology based solutions as well as industry collaboration and education are also required, which is further outlined in this response.

There is also increased pressure on ISPs to provide solutions and a greater degree of consolidation within the solutions market, as well as growth of partnerships offering wider solutions integration.

Beyond anti-spam technology and legislation, vendors and industry bodies must continue to work on alternative solutions to the spam problem.

1) The extent of the problem.

Junk email began as little more than a nuisance in the early 1990s, initially frowned upon as being somewhat unethical, but not such a problem that anyone felt the need to do anything about it. Since then, spam has grown exponentially to become a serious threat to email security for businesses all over the world.

By 1999, the proportion of spam turning up in corporate mailboxes was already becoming a concern. And by early 2003, the sheer volume of spam had become so damaging that most businesses were finally forced to wake up and search for new ways to control the escalating problem.

Figures for 2003 have shown the global escalation of spam volumes in an alarming perspective. In January 2003 MessageLabs statistics were showing that 1 in every 4.1 (24.4 per cent) emails was identifiable as spam. By May, spam accounted for 55.6 per cent of email traffic, in December this figure rose to 62.7 per cent, and in early 2004, spam still accounted for around 60 per cent of all email traffic.

In September 2004, MessageLabs scanned more than 1.45 billion emails worldwide for spam, of which over 1.05 billion or 72.14% (1 in 1.39) were stopped as spam (404.68 per second).

Market researcher Ferris Research reported that spam cost US businesses US\$10 billion dollars in 2003, an increase from \$8.9 billion dollars in 2002. Ferris estimated that as much as 40 per cent of these losses were accounted for through lost productivity. Office workers were estimated to spend around 4.5 seconds reviewing and deleting each email message. The additional consumption of bandwidth and rising technical support overheads also accounted for part of these rising costs.

Ferris also estimated that spam cost EU businesses approximately US\$2.5 billion dollars, and the European Commission's own figures suggested this figure was in the order of 2.25 billion euros. Moreover, in 2002, spam only accounted for around 20 per cent of all email traffic, so the overall figure is set to rise sharply. In 2003, MessageLabs estimated that British businesses had lost around GB£3.2 billion in productivity costs related to the effect of managing spam in users' inboxes. When factoring in other costs, such as bandwidth problems and managing addition server capacity, the true cost becomes much higher.

The threat to Internet Service Providers (ISPs), businesses and consumers is particularly severe in the US. One large ISP reported receiving nearly two million spams each day from a promotions company until an injunction was obtained to prevent it. Even given the assumption that each user spends only a few seconds identifying and deleting spam messages, the amount of connection time being squandered through that single ISP was in the order of 5,000 hours every day.

2) Pros and Cons of a legislative approach.

Already it is clear that having a legal framework is only part of the solution. While laws may make it less appealing and more difficult for a spammer to operate and be profitable, there will always be a need for technical solutions as well.

There are clearly major differences between legislations around the world in place today. For example, the EU, Australian and US legislation are different in terms of opt-in vs. opt-out requirements. The US law is unambiguously opt-out, requiring recipients to reply to emails in order to stop receiving email communications. On the other hand, the EU and Australian legislation stipulates that individuals (and businesses in certain countries) have to opt in before they can be sent commercial emails. Because the vast majority of spam is generated in the US, much of this spam will fall under the opt-out principle.

The plain fact is that laws in themselves will never defeat the determined criminal or shady operator. The "locks" needs tightening up too. The only way to be certain of combating the growing menace of junk email is to put in place an intelligent security system which can identify spam accurately and stop it at the Internet level — before it can get anywhere near your network boundaries and start clogging up your email system.

Despite the fact that many spam experts have already dismissed the US' CAN-SPAM Act as largely ineffectual, there is some evidence that the spammers themselves are beginning to take notice of anti-spam legislation. In a recent New York Times interview with Alan Ralsky, widely acknowledged to be

one of the most prolific spammers in the world, he says that although he will not stop sending bulk email, he will change his processes to ensure that he complies with the new law.

Whilst on the surface this seems to be a good thing, it is statements such as these that reinforce the view that the law actually helps to legitimatise spam, rather than outlaw it.

Soon after its introduction into federal law, the CAN-SPAM Act was given an early run out by a group of companies with a vested interest, including AOL, Earthlink, Microsoft and Yahoo! Around six lawsuits were filed and 118 spammers were being pursued under the new legislation. The case was being brought against some of America's most prolific spammers, with only a handful actually named, the majority were cited as "John Doe", whose true identities would hopefully be later revealed. The allegations were that these spammers were in breach of the new law, by making use of "open proxies", having false return addresses, having no provision for unsubscribing, and not including a physical mailing address.

Hardened spammers like Ralsky are seemingly prepared to tailor their practices in order to comply with new legislation, and as yet no spammer has come forward to say that the law will proactively result in them shutting down their business. Although the Direct Marketing Association recently announced that as a result of the CAN-SPAM act, the cost of reaching consumers through email direct marketing activities has increased, and response rates are down.

Since the new legislation was introduced in the US in January 2004, AOL has suggested that the volumes of spam it has had to deal with have dropped considerably in recent months. The company says they have seen a 27 per cent decline between February and March 2004. On 20 February, 2.6 billion spam emails were stopped, but this figure declined to 1.9 billion on 17 March.

During this same period, AOL also saw the number of complaints from its subscribers about false negatives not being stopped fall by almost 50 per cent, from 12.7 million to 6.8 million.

MessageLabs' own statistics also bear this out. For example, had the volume of spam continued to increase at similar rates to those monitored in December 2003, it would likely have accounted for 80 per cent of all email traffic by mid-2004, but the figure actually dropped from 63 per cent in January to around 53 per cent in March.

Although it is still too early to draw definite conclusions, the global figures have noticeably diminished, perhaps as a result of the effects of new legislation in the US, Australia and within Europe. With improved anti-spam filtering techniques, only time will tell if legislation has any sustained effect.

3) Industry cooperation and anti-spam awareness initiatives

Consumers, businesses, legislators, law enforcement and industry groups are all working to fight spam, primarily owing to its staggering billion-dollar economic costs.

MessageLabs strongly believes that industry cooperation is important in the fight against spam. MessageLabs works closely with the Anti Spam Research Group (ASRG) set up by the Internet Engineering Task Force (IETF) in the US, the Internet Industry Association (IIA) in Australia and the HKISPA in Hong Kong amongst many others around the world, in the pursuit of research into the legal issues of spam, to understand the problems it poses and to come up with thoroughly evaluated solutions.

Beyond anti-spam technology and legislation, vendors and industry bodies continue to work on alternative solutions to the spam problem. One of the latest ideas has come from Microsoft, and is based upon the postage system introduced in Britain in 1830s. Appropriately enough, it is called the "Penny Black" project. The aim of the project is to shift the cost burden of emailing spam to the sender rather than the recipient.

The form of "payment" would most likely be the amount of time it takes a computer to perform a particular task. For example, before an email was sent to a new email address the machine would take around 10 seconds to solve a "cryptographic puzzle". Once the puzzle is solved the email can be sent. The theory is that the recipient can then add the sender to a whitelist, because they know that someone has spent a degree of time and effort in sending the email to them personally.

The main advantage of such a system would be that spammers would see a massive increase in the time it takes to send bulk email. Instead of being able to send out millions of messages, a 10-second delay would see a single computer limited to around 8,000 emails per day. The extra computing power, time, and effort would mean spamming would be much less effective as a means of income.

There are, however, disadvantages to this kind of approach. Just because someone has gone to some degree of effort to send an email does not necessarily mean that the recipient wants to receive it. Also, a system such as this would need to be based on open standards not proprietary to Microsoft, and would require a radical overhaul of the global email infrastructure.

4) Technical solutions

There are a number of methods that can be employed to fight off spam, some more effective than others. Broadly speaking they are as follows:

DNS (or IP) blacklisting.

This was the first spam prevention mechanism to be deployed. It is simply the blacklisting of known spammers, enabling any communication coming from a blacklisted IP address to be blocked. Its weakness is that, once the spammer knows the address he is using is blacklisted, he simply moves on to a new one. Additionally, blacklisting only filters on the basis of IP address, without analysing the textual content of the email itself.

Historically, blacklisting has tended to result in a high degree of false-positives, where legitimate email is wrongly identified as spam. However, as the technique has matured, this problem is thankfully no longer on the same scale.

Fingerprints or signatures.

As in the case of viruses, it is possible to generate what are known as signatures or “hashes” of any particular bulk-mailed spam outbreak. This fingerprint can then be loaded on to an elementary spam filtering system, which will then stop all email bearing that signature. The technique results in practically zero falsepositives, but it suffers from the “sacrificial lamb” problem.

In other words, somebody has to get hit by the particular spam before it can be analysed, its signature created and then made available. The problem is that it is relatively easy to defeat such a “hashed” signature, by injecting each instance of a spam email with some random text or numbers, for example. This is a technique known as “hashbusting,” and only a fuzzy-fingerprint system capable of detecting these hash-busters will succeed.

Whitelisting.

This is like blacklisting in reverse. The idea is that only mail which is sent to you by someone who has already contacted you by email can be delivered into your inbox. Any first-time correspondent who is not on your whitelist must identify himself before the mail can be accepted. This can create irritating problems, however. For example, if you buy some product or service from an online store, how does the automated confirmation of receipt get through your whitelisting system?

Collaborative filtering.

This method relies on the goodwill of anonymous Internet users who upload details of spams which they've identified — and may well have been hit by — to a central web site. A number of anti-spam services use this databank of user submissions as the basis for spam detection, but unfortunately the method is beset by high numbers of false positives.

Heuristics.

Essentially heuristical analysis revolves around a complex set of rules that can be combined to identify what is and what is not spam. It's a technique that MessageLabs developed with enormous success in identifying email-borne viruses and has further exploited in its anti-spam technology. Heuristical methods alone are no longer a complete safeguard in combating spam, however, since the spammers are improving their technique in making spam look more like genuine email. Heuristical analysis is now only one weapon in the armoury and is often used to identify spam-like emails in combination with other techniques, such as statistical analysis.

Bayesian probability.

At MessageLabs we have pioneered the use of mathematical machine learning techniques in identifying spam. Bayesian probability assesses the statistical likelihood of an email being spam by learning to recognise the difference between bona fide emails and spam. Simply, the more email that the engine sees, the better it becomes at spotting the spam.

Bayesian probability models have proved to be extremely powerful and effective — reducing the false-positive rate to an almost negligible one in 1,000 incorrectly identified emails. As a consequence, spammers have adapted their methods, seeking to improve the statistical probability of their spam appearing more like a non-spam email. This has become known as “stats-busting”.

URL Signaturing

Another technique for combating spam is through a mechanism called “URL signaturing”. This is used to block the spam based on the URL of the domain which is being spamvertised within the email itself, rather than blocking based on the IP address from which the spam is sent (which can be an open proxy). This means that the mail software must be capable of parsing the URLs within an email and using that to match against the URL signature database.

The URL signature database can be populated from a network of honeypots, and it already very successful at identifying spam. This is a technique that MessageLabs has pioneered and developed using proprietary technology.

However, it is highly likely that this type of mechanism will become more widely adopted in other anti-spam solutions, using a variety of plug-ins and DNS blacklisting services to achieve the same results.

Haiku.

Developed by the Habeas Sender Warranted Email (SWE) programme, a more recent method that is now becoming more widely used is one in which the proprietary “Haiku” tag is licensed and included in the email headers using special Xheader tags.

The Haiku, which consists of a small poem akin to a traditional Japanese form of poetry, can be used to indicate a pre-existing relationship, for example. "Copyright does not protect names, titles, slogans, or short phrases," says Habeas, "it does protect poetry." The aim of this is therefore to make mail filtering much simpler by further eliminating the numbers of false-positives. It is also intended that should a spammer misappropriate the Haiku tag, copyright laws can be used against them, as Habeas has promised to sue anyone who includes the Haiku in a spam email. However, it remains to be seen how successful this approach will be in the longer term, and it has many critics as well as supporters.

The potential licensing costs may put some people off, although it may offer a guarantee that the message will get through. The approach also employs a whitelist and blacklist that lends support to the overall process, as SWE licensees are whitelisted, consequently, abusers are also blacklisted. Some spammers have chosen to ignore these legal risks and are already being sued by Habeas – poetic justice, perhaps.

5) Emerging Technologies – sender authentication.

Simple Mail Transfer Protocol (SMTP) is the protocol used to send email over the Internet. SMTP is used for outgoing email while POP3 is used for receiving email. At its most basic level, sender authentication is a way to check that an email has genuinely been sent from the user or domain it claims to come from. This can be done by examining the IP address the email has been sent from. If the IP address does not match the sources of email as given by the domain it is likely to be a forgery. IP addresses should be unique for each computer that is connected to the Internet, which makes it very difficult to forge an IP address when actually delivering an email.

What is sender authentication?

It is important to note that sender authentication is not a way to prevent spam. It is a way of finding out whether an email has been forged (or spoofed). If it has been forged, then that is a strong indicator that the sender is a spammer.

Sender authentication serves two main purposes: firstly, to prevent bounce-backs to people who it is claimed sent a particular email when in fact they didn't. Secondly, as a basis on which to build stronger trust relationships with the sender.

The problem with SMTP as it currently stands is that it is completely anonymous on the sender-side of the conversation. Potentially, anyone can send a message to a valid recipient, and forge the sender's "from:" address. This has now become common practice, particularly for spammers and virus writers wishing to hide their identity.

How does it work?

A company with the domain name example.com would publish a list of IP addresses from which messages from example.com may be sent. Any email claiming to be sent from example.com could then be checked against this list to ensure that the IP addresses match one of those published for that domain. If an email is delivered from an IP address not in that list, which still claims to be a sender in the example.com domain, there will be a discrepancy and the message may not be trusted.

There are essentially three main technologies that can provide sender authentication:

Sender Policy Framework (SPF) – has been created by pobox.com, one of the largest US-based email forwarding services. It is currently being trialled by AOL and is probably the most well-established of the sender authentication systems. It has the backing of much of the industry; it works and already has around 10,000 domains registered. The main problem with SPF is that it currently breaks certain kinds of email forwarding, which means that you have to switch from "forwarding" to "re-mailing".

DomainKeys – This is Yahoo's proposal for sender authentication and is a more complex offering than SPF. The proposal is still being formulated, although basic details are known. The main difference is that DomainKeys validates an individual email rather than a sender. It is however potentially fragile due to emails being re-written by certain types of gateways (eg: mailing lists), causing the DomainKeys signature to be invalidated.

Caller-ID – Microsoft has only recently made their offering public. This is similar to SPF in that it tries to validate the sending domain, but is based on the headers of an email rather than the SMTP envelope (which is the conversation that takes place on the email server when delivering an email). This makes implementation more complex and more fragile, it also means there will be no saving in bandwidth with Caller-ID as there is with SPF. Caller-ID also means that all email clients have to change, which is a major undertaking.

Caller-ID has fewer features than SPF, and may appear to be a less well thought out specification. However, the backing of such a major player as Microsoft is likely to heavily influence adoption of Caller-ID.

Is sender authentication being used now?

Although sender authentication is not being used extensively at the moment, MessageLabs will additionally offer support for these technologies as the demand increases. This is still a relatively new area, and uptake is likely to increase significantly in 2004. However, for it to work effectively, sender authentication needs mainstream support amongst users, and given the current spam climate this is a distinct possibility.

6) The MessageLabs anti-spam service

As a highly focused, specialist managed service provider, MessageLabs is a world leader in all aspects of email security. Our anti-virus service, which stops all known and unknown viruses before reaching our customers' networks, is already protecting thousands of corporate users from the ravages of email-borne infection. We also provide an image filtering and content control service, which spares our customers many of the problems that adult oriented emails and attachments may cause.

At the core of our anti-spam service is a learning engine containing more than 1,000 rules, overlaid by artificial intelligence techniques based on statistical probability, similar to those already used for determining the probability of certain illnesses in patients.

MessageLabs has pioneered these established techniques in combating spam by searching for particular patterns and characteristics within large volumes of junk email, and we have found this to be very successful in almost eliminating the numbers of false positives. Currently the MessageLabs combined approach is more than 90 per cent accurate, only seldom mistaking legitimate email for spam. The MessageLabs service is unique in that it allows for set up and fine-tuning of personalized filtering criteria, using a combination of public and internal white and blacklists. It also enables the user to specify how all spam and suspect email is to be handled — whether quarantined in a designated safe inbox or disposed of on receipt at MessageLabs. This helps to free up users' time, as well as alleviating bandwidth issues and reducing the demands on internal email systems for storage space.

MessageLabs Spam Manager quarantines messages identified as spam in a location accessible for review by an organisation's employees. By the use of Spam Manager, users are able to view and release messages to their regular email in-boxes, delete messages and manage individual Notification, Email Address and Password options.

7) Conclusion - Combined solutions for the future

In 2002, in excess of 64 million spam emails were identified and intercepted by the MessageLabs anti-spam service on behalf of our customers. In 2003 this figure rose to 1.2 billion. The evidence is all around that the spam menace is becoming ever more of a problem for business email systems. Indeed, whether you measure the problem by your own experience of mounting spam incursions in your own inbox or by global statistics that track the massive rise in spam volumes, the picture is clear: the spam problem is getting worse almost by the day; and it is certainly not going to go away in the short term.

Before too long, the explosion of spam filling our mailboxes will significantly reduce the effectiveness and efficiency of email as the most widely used Internet application, damaging the credibility of the medium as one of the most powerful business applications we have come to know and rely on.

The most prominent irony of the spam epidemic is that, in the longer term, the spammers are simply killing off the very medium on which their activities depend. By flooding the marketplace with their wares in such enormous volumes, they are rapidly throttling the email system — like a parasitic ivy plant, which eventually smothers the tree it invades.

The determination of spammers to continue plying their dubious trade can be seen from the increasingly devious methods they are employing in order to defy anti-spam measures. Meanwhile, systems which deploy only one or another anti-spam technique have already been rendered obsolete as the spammers find their way round them.

It is likely that effective anti-spam technology will remain the most successful way of combating spam, although over time other measures will probably make an increasingly valuable contribution. A combination of effective anti-spam technology, appropriate and informed legislation, a proven ability to implement that legislation, cooperation on the part of industry vendors and bodies and user awareness are all needed if the scourge of spam is to be decisively challenged.

It is unlikely that the laws we have now will change significantly over time, but the avenues for enforcement, regulation and investigation will perhaps evolve as understanding of policy effectiveness, enforcement and spamming techniques develops. The opt-in vs. opt-out debate between the EU and the US, for example, will only be resolved by closer cooperation between parties such as the US FTC and the UK Department for Trade and Industry (DTI).

In any event, a technical solution will be the cornerstone of any effective attempt to tackle the problem in reality, with the majority of spam originating from the US and from other countries with even fewer restraints. The differentiator between competing technical solutions will not be so much their ability to filter spam, but on the number of false positives that are incurred. The balance of cost in lost productivity will shift from managing users inboxes to managing the spam quarantine bays, and this could become the killer for some solutions.

Spammers are already finding new ways to circumvent the statistical filtering methods, and as we have already seen, they are becoming more sophisticated. As this level of sophistication improves, the

only way to combat the problem will be to employ a combined approach to combating spam. At MessageLabs we believe that the only way to combat spam comprehensively is by combining the best of all antispam techniques into an intelligent whole. The only way that we can preserve email as the vitally useful communications medium it has become is to prevent the “ivy” from taking hold in the first place. The fact is, the menace of spam can only be contained by proactively safeguarding email systems from the damaging effects of unsolicited mail — and that means putting in place the most comprehensive defence system possible.