

Is the end nigh for spam?

In our last examination of the spam situation a year ago, we suggested the notion that legislation alone could rid the world's email inboxes of junk mail was pure 'spamtasy'. Twelve months on, while the rush towards introducing legislation continues, global legislators and industry players are also slowly coming around to this view. In the words of the International Telecommunications Union (ITU), there is no silver bullet to curb spam: legislation alone cannot kill it.

So are we any better off today, than we were 12 months ago? Since most spam comes from the US, we take a fresh look at what's happening round the globe to curb the problem.

US

The CAN-SPAM Act was signed into law by President Bush on 16 December 2003, and came into force on 1 January 2004. The CAN-SPAM Act requires that unsolicited commercial email senders:

- ensure that the 'from' line accurately reflects the sender's identity;
- include a subject line that is consistent with a message's content;
- include a valid postal address;
- include a working opt-out /unsubscribe mechanism as a way for the consumer to decline to receive further commercial emails from the sender;
- do not use Internet-crawling software programs to harvest email addresses for spamming; and
- send spam using an intermediate computer without the owner's knowledge or consent.

The Act also permits damages of up to \$2m against companies that violate the provisions of the law, which can be trebled by a federal district court if it determines that a violation is wilful or meets other specific conditions.

The Act also instructed the FTC to put forward plans, within six months, for the introduction of a national 'do-not-spam' list. In June, the FTC told the government that this would be problematic from privacy and technological standpoints, and would almost certainly increase the amount of spam individuals received by providing a list of 'live' email accounts. Instead, the FTC recommended the widespread adoption of email authentication standards.

The problem with the Act is basic and therefore ironic -- it fails to actually 'can' spam. By adopting an 'opt-out' approach, which has been shown to be highly ineffective in other states and countries, the Act does not actually ban sending spam at all; what it does instead is tell spammers how to present their spam to comply with the law. As long as it is labelled correctly and recipients are given a means to opt out, then companies may spam away. Yet despite this it has been estimated that CAN Spam Act compliance has been as low as 1 per cent (current figures suggest 4 per cent).

The 'Coalition Against Unsolicited Commercial Email' stated:

'This legislation fails the most fundamental test of any anti-spam law, in that it neglects to actually tell any marketers not to spam. Instead, it gives each marketer in the United States one free shot at each consumer's email inbox, and will force companies to continue to deploy costly and disruptive anti-spam technologies to block advertising messages from

reaching their employees on company time and using company resources.'

Cases

The Act has seen its first conviction. A Californian man, Nicholas Tombros, pleaded guilty in September this year of sending pornographic spam, by driving around Venice beach looking for unprotected wi-fi hot spots. In addition, the Federal Trade Commission (FTC) has already filed over 60 spam-related cases against individuals and companies. In April, it filed its first two cases under the CAN-SPAM Act, against Phoenix Avatar and Global Web Promotions Pty Ltd.

In May 2004, District Judge James Holderman issued a temporary restraining order against Phoenix Avatar, freezing the company's assets and ordering it not to send spam emails. The FTC had charged Phoenix Avatar with sending illegal spam, by using innocent third party email addresses in the 'reply-to' or 'from' fields (spoofing), and by providing no means for recipients to opt-out/unsubscribe from the emails.

The FTC also charged Global Web Promotions Pty Ltd, Michael John Anthony Van Essen, and Lance Atkinson with violations of the Act. Global Web was accused of marketing a diet patch and other anti-ageing products, and using spoof email addresses. As Global Web is an Australian company, the FTC obtained a preliminary injunction against 'fulfilment houses' in the United States preventing its delivery of Global's products.

These are not the only instances of legal action being taken: in April last year the Department of Justice filed a criminal complaint against four men from Detroit accusing them of mass spamming. Another man was ordered to pay Microsoft \$4m for allegedly sending millions of emails appearing to be from Microsoft; and the Massachusetts Attorney General Office filed suit against Florida man in July.

In late October 2004, the world's major ISPs launched a new round of lawsuits against alleged spammers under both the CAN SPAM Act, and other federal and state laws.

- AOL sued unnamed defendants for sending spam messages for control prescription drugs. This lawsuit, filed against ten 'John Does', is also noteworthy because it is the first time AOL has filed a spam lawsuit based on a large number of complaints specifically determined to be from AOL Europe and AOL Canada members. It also filed against a further twenty unnamed defendants for sending unwanted communications to online consumers via instant messaging tools or chat rooms.
- Yahoo sued two pornographic content providers, Epoth and East Coast Entertainment Group, accusing them of unlawfully disguising their identities, sending anonymous emails with sexually explicit subject lines without an option to opt out or unsubscribe from further emails.
- Microsoft filed three lawsuits against unnamed defendants alleging that defendants spoofed the domains of all four ISPs and used open proxies to route the emails advertising herbal medications and cheap mortgages.
- Earthlink filed suit against 50 unnamed defendants the company accused of sending spam advertising prescription drugs, and cheap loans.

State Law

The Majority of US states now have some kind of spam legislation. Maryland's new The Spam Deterrence Act based on Virginia's law, makes it illegal to use false header information; and imposes fines up to \$10,000 and three years jail time for first time offenders, and \$25,000 and jail time of up to 10 years for repeat offenders. The law also allows monies made from the spamming to be taken by the state.

Virginia is regarded as having the toughest of all the state laws, so it is appropriate that this was the scene of the US's first felony convictions for Spam. In November 2004, a Loudon County jury, convicted Jeremy D Jaynes and his sister Jessica DeGroot, for sending spam to Virginia residents. The Jury recommended that Jaynes, regarded as the eighth-worst spam distributor in the world at the time of his arrest in December 2003, was sentenced to nine years in prison, while DeGroot was fined \$7,500.

The Prosecution told jurors that on one day alone in July 2003 they sent, or attempted to send, 7.7 million email messages to AOL customers using bogus company names and false identities.

Jaynes was convicted of sending spam messages (exceeding 10,000 messages during each 24-hour period) and offering goods that did not exist. The indictment also alleged that the Jaynes had falsified transmission or routing information to prevent recipients from knowing who had sent the messages and how to contact the sender. In one month alone, Jaynes received 10,000 credit card orders, each for \$39.95 for one product alone. According to prosecutors, Jaynes had amassed a fortune of \$24m from his sales.

Although both Jaynes and DeGroot lived in North Carolina, Virginia asserted jurisdiction because they sent messages through America Online server computers located in the state, and charged the defendants with violating Virginia's anti-spam law. The law, approved in March 1999, makes it illegal to send unsolicited bulk email containing falsified routing information if the sender thereby violates a provider's policies or distributes software designed to falsify routing information. The law was amended in April 2003 to increase the penalties for sending a high volume of messages containing falsified routing information.

Jaynes and DeGroot will be sentenced by Circuit Court Judge Thomas Horne in February. He will have the option of reducing the jury's sentence. Perhaps more interestingly, Horne has not yet ruled on an earlier motion before the court to dismiss the whole case.

Rest Of The World

China

China's effort to control its citizens' access to the Internet and in particular its censorship of outside content, is well known. Less well known is that over the past 12 months it has become one of the world's spam havens, with an estimated 70 per cent of all the world's spam advertising websites hosted in China.

The choice of China should not be a surprise, as for the time being sending spam remains legal in China, and so the government has little current interest in going after anyone sending such material -- especially if they are not targeting Chinese citizens. The vast majority of credit card fraud, phishing scam sites are now also being hosted on Chinese servers, most of which are owned by state telecom operator China Telecom's subsidiaries.

China, however, does not want to look like it is uninterested in the problem to the outside world and it is believed that the Ministry of Information is preparing an anti-spam bill for introduction sometime in 2005.

Australia

It can be no coincidence that the 'opt-in' Australian Spam Act of 2003 has been hailed as the world's best and most effective piece of anti-spam legislation. The Spam Act came into effect on 10 April 2004. Following it, Spamhaus reported a notable drop in the activity of known Australian spammers since the law's introduction. The Act provides for penalties of \$1.1m a day for professional spammers. The SPAM Act regulates commercial electronic messages ('CEMs') by providing that, subject to limited exceptions, they:

- must not be sent without the prior consent of the recipient. (That consent may be express or implied -- 'reasonably inferred' -- from the conduct, business and other relationships of the person or organisation concerned);
- must contain a functional unsubscribe facility; and
- must accurately identify the sender of the message.

The SPAM Act also prohibits the use of address harvest software, as well as the lists generated by such software.

The Act draws a distinction between 'commercial electronic messages' (CEMs) and 'designated commercial electronic messages' (DCEMs), which the Act does not prohibit. A DCEM is defined as a message that only contains factual information and certain additional information about the sender of the message, but only if the message would not constitute a CEM without that additional information.

Electronic messages from government bodies, political parties, religious organisations, charities or educational institutions are exempt from the regulations and classed as DCEMs.

Australia's close neighbour, New Zealand, currently without a spam law, looks set to follow Australia in adopting a tough opt-in anti-spam law early in 2005.

EU

The European Commission published a communication in January 2004 that aimed to help enforce the Privacy and Electronic Communications Directive.² The communication focused on effective enforcement by member states, technical and self-regulatory solutions by industry, consumer awareness and international co-operation. It identifies a series of actions required to complement rules established by the Directive in order to make the ban on spam as effective as possible. This includes:

- providing competent authorities with suitable investigative and enforcement powers to trace and prosecute 'spammers'; and
- adapting marketing practices to the 'opt-in' regime, explaining to users how to avoid spam and the benefits of filter software and security.

The Commission also issued a questionnaire to gauge how effective the current regime has been. The Commission has called in Spamhaus director, Steve Linford, to advise the Commission on possible new legislation to better tackle the spam problem -- and to consolidate the various anti spam measures contained in Distance Selling Directive, E-Commerce Directive, and Privacy and Electronic Communications Directive. Linford, wants to see Europe adopt a law similar to the Australian anti-spam

law. 'We are recommending that Europe uses the Australian law as a template. That's the best one so far. It's working because it penalises spammers.' Quote taken from Zdnet.

UK

In the UK, the Privacy and Electronic Communication regulations, which came into force in December 2003, make it illegal to send an unsolicited email to anyone with whom the sender doesn't already have business relationship. The regulations which only cover personal email addresses, not business email addresses, are already being seen as a failure. The Information Commissioner's Office, which has responsibility for enforcement, admits that whilst they have already received complaints from many UK citizens, it is not in a position to take action speedily due to lack of resources and powers. The Information Commissioner's Office wants the government to grant it 'Stop Now' powers to prevent those being investigated from sending further spam.

The UK's domain name registrar, Nominet, recently obtained an injunction against the UK's alleged biggest spammer, Peter Francis-Macrae. Nominet alleged he had been sending fraudulent re-registration letters to domain holders asking them to pay his company. He has also recently started a company taking advance orders for .eu domain names.

Netherlands

In the Netherlands, the Dutch telecommunications regulator, OPTA, and the data protection agency, CBP, signed a joint agreement on 19 October to begin sharing information and co-operate more in fighting spam. The agreement followed on from requests from the Dutch Lower House and ministry of economic affairs who have been pushing for these two agencies to work closer together in the country's battle against spam.

In March 2004, the Dutch Supreme Court ruled in a spam case that XS4ALL, a Dutch ISP, was allowed to block the delivery of spam over its network. The court, in finding against Abfab's claims that its free speech was being impinged stated:

'Anyone who without authorisation makes use of property to which another party has an exclusive right, and who thereby infringes that exclusive right, is acting unlawfully vis-à-vis the beneficiary of the right, unless there is justification. The right to freedom of speech does not constitute such justification. This fundamental right cannot serve in principle to justify transgressive use of property to which another party has exclusive rights.'³

Based on this judgment, all providers in the Netherlands have the right to impose an *a priori* ban on the sending of spam, even when addressed to their business customers. This judgment, therefore, goes further than the Netherlands' anti spam legislation (implementing the EU Privacy and Electronic Communications Directive) which, like the UK law, only forbids the spamming of private email addresses but leaves business email addresses unprotected.

Germany

The Higher Regional Court of Düsseldorf held that the sending of one spam email gives rise to a valid presumption that more will follow. The presumption will, however, be negated when the spammer signs a cease-and-desist declaration. The court also ruled that a spammer is only able to legally send advertising email when he has the express or implied consent of the recipient. A potential interest in the advertisement alone will not constitute a valid ground for sending the email. See OLG Düsseldorf, Decision of 22 September 2004.⁴

Having surveyed what the world is doing to declutter our inboxes, the next instalment of this feature looks at the technological solutions put forward to eliminate spam -- and the new threats facing technology.

* * * * *

At an ITU world summit on the information society meeting at Geneva, in July 2004, the delegates heard that 76 per cent of all email was now spam, costing the world's national economies around US\$25bn a year. The delegates concluded that the only effective way forward in the fight against spam was with a combination of strong legislation, technical solutions, consumer education, industry self regulation, and global co-operation between countries and organisations.

* * * * *

¹ http://www.mxlogic.com/news_events/10_08_04.html

² http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

³ <http://www.xs4all.nl/uk/news/overview/abfab120304fv.html>

⁴ <http://www.jurpc.de/rechtspr/20040261.htm>

