Legal update

Getting tough on spam?

Received: 6th April, 2005

Ewan Nettleton

is a solicitor in the Intellectual Property Department at Bristows. He specialises in intellectual property law. He has an MA in chemistry and a D.Phil in protein chemistry.

Abstract Recent estimates suggest that spam now accounts for as much as 60 per cent of all global e-mail traffic,¹ ranging from business advertisements to outright fraud. The EU and USA have recently introduced anti-spamming legislation — implementation of Directive 2002/58/EC in the EU and passing of the CAN-SPAM Act in the USA respectively. This paper looks at the difficulties inherent in legislating against spam and assesses how successful the recent legislation is likely to be at stopping the spammers. It also considers the effect the legislation is likely to have on legitimate marketing companies.

INTRODUCTION

Recent estimates suggest that spam now accounts for as much as 60 per cent of all global e-mail traffic,¹ a statistic all too evident to most e-mail users. The content of such e-mails ranges from unwanted business advertisements to attempts at downright fraud. A recent example at the latter end of the scale purported to be from the lawyers of the late Sir Dennis Thatcher, and sought to dupe recipients into thinking they would receive just short of £1m on providing identification information needed under UK inheritance law.² This is an example of so-called 'phishing', a technique used to lure naïve respondents into providing contact or banking details which are then used to extract money from their bank accounts or to create stolen identities.

In December 2003, the UK Regulations³ implementing the Directive on Privacy and Electronic Communications (2002/58/EC) — the

centrepiece of the EU's armoury of recent anti-spam legislation — came into effect. These have been described in Nettleton⁴ and Nettleton and Phram.⁵ The Directive has also been implemented in many of the other member states of the EU, although the means of its incorporation into the national laws of individual countries has varied. The United States' CAN-SPAM Act took effect in January 2004, and other countries around the world (eg Australia) have also recently introduced anti-spam legislation.⁵

It is now over a decade since spam e-mails first started arriving in our inboxes,⁶ yet the new legislative regimes in Europe and the USA are now just over a year old. This paper takes a look at the present state of the global spam problem, and assesses the extent to which the new laws are succeeding. Some of the other non-statutory initiatives being taken around the world are also considered.

Ewan Nettleton

Bristows, 3 Lincoln's Inn
Fields, London WC2A 3AA,
UK.

Tel: +44 (0)20 7400 8000;
Fax: +44 (0)20 7400 8050;
e-mail: ewan.nettleton
@bristows.com

PROBLEMS AND PROLIFERATION OF SPAM

E-mail spamming is a global problem. It has arisen principally because e-mail, by contrast with other more traditional means of relaying information, is (once appropriate systems are in place) virtually free to send and capable of reaching a huge target audience, across all corners of the globe. This means that the spammers' activities can be commercially viable even though the take up rate from spam e-mails is relatively small.⁷

Although e-mail users worldwide feel the effects of spam, the vast majority of it is thought to originate from a small number of discrete sources. Indeed, it has been suggested that 80 per cent of the spam received by internet users in North America and Europe is sent by a mere 200 spamming outfits comprising 500–600 professional spammers.⁸ Recently, an individual was arrested in the USA, accused of sending a staggering 1.5 million spam e-mails.⁹ The geographical distribution of spammers is also far from uniform; a recent study suggests that over three-quarters of the world's spam comes from just five countries, with over 40 per cent of it originating in the USA.¹⁰

This background makes the legislators' objectives of reducing spam intrinsically difficult, because in most cases it will originate from outside their jurisdictions from a small number of dedicated spammers who are unlikely to pay heed to any new laws. It also provides a difficult environment for respectable marketing companies, which have to deal with the regulations imposed to curb spam and to differentiate themselves from the spammers and their overly intrusive practices.

UK REGULATIONS AND THE EUROPEAN DIRECTIVE

The UK Government implemented Directive 2002/58/EC (via the

Regulations) with effect from the end of 2003. Although the majority of the other EU member states have also now implemented the Directive, there are still some exceptions.¹¹ The Commission is still in the process of examining the new laws enacted to check their conformity with the Directive and has started legal proceedings against some of those member states who have not implemented it.

Indeed, there are differences in the ways in which the Directive has been implemented in the member states which have adopted it — some of which at least stem from the different options for implementation available under the Directive itself. One notable example concerns whether or not 'legal' persons such as companies (as opposed to 'natural' persons such as individuals) have to 'opt-in' before they can be sent legitimate unsolicited direct marketing communications. Commentators have suggested that the UK's Regulations take a soft approach. The UK, like France,¹² — which is thought to be Europe's leading source of spam,¹² — Portugal, Austria, Iceland, Sweden and Finland,¹³ has adopted an opt-out model for legal persons, meaning that they can, subject to other general requirements for compliance being fulfilled, be sent unsolicited e-mails without their prior consent having been obtained.¹⁴ It has also been suggested that the penalties for non-compliance are too lenient in the UK and that enforcement is ineffective.¹⁵ This contrasts with member states such as Italy, which has implemented legislation that adopts the opt-in regime for legal persons (as well as for natural ones)¹⁶ and imposes significant fines and even jail terms for persistent spammers.¹⁷

Given the difficulties identified above, it is hardly surprising that the Council of the EU has recently invited the Commission to evaluate whether the

differences in national laws on privacy and electronic communications, including those which have arisen from implementing the Directive, could represent an obstacle to effective cross-border enforcement. Similarly, these problems may also explain why the Council is seeking to encourage other anti-spamming initiatives such as cooperation on enforcement and exchange of information within the EU and the investigation of other solutions aimed at combating spam.¹⁸

THE US CAN-SPAM ACT

In the USA, which, as noted above, is thought to be top of the league when it comes to sources of spam, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act has been in force since 1st January, 2004. This federal US legislation followed a number of earlier anti-spam Bills considered by the US legislature over several years¹⁹ and is specifically aimed at curbing the problem. The regime it introduced was completely opt-out, however, meaning that unsolicited e-mails could be sent without consent to natural persons as well as legal ones (by contrast with the EU Directive, which provides an opt-in regime for natural persons), though it should be noted that some US states (most notably California) have stricter state laws regarding spam. This and other aspects of the legislation have led to vocal US anti-spam activists deriding the new legislation, which some now refer to as the 'You-Can-Spam' Act.²⁰ Some have even suggested that the Act compounds the problems of spam, by encouraging unsuspecting recipients to click on opt-out or unsubscribe links in unwanted e-mails, which, for spam at the lower end of the reputability scale, could be dangerous.²¹

That said, there have been some successes. For example, a case has been recently settled between the US Federal Trade Commission (FTC) and a company accused of sending millions of illegal e-mail messages marketing bogus diet patches. The FTC claimed that the company had breached a number of federal US laws including the CAN-SPAM Act. According to the FTC, the settlement bars the defendants from violating CAN-SPAM; from making false or misleading claims about their products or services; and from making unsubstantiated health, efficacy or safety claims.²² There have also been a number of other high profile US anti-spam cases.²³

OTHER INITIATIVES

In addition to the legislative changes, several other anti-spam initiatives are being taken around the world. On the technical side, methods of filtering e-mails are becoming more sophisticated and individual companies are, through use of appropriate IT systems and internal procedures, taking steps which seek to minimise the volumes of spam that get through. Techniques include:

- Blacklisting — This involves rejecting e-mails from particular blacklisted sources; eg through subscribing to particular lists of spam sources set up for that purpose. It does, of course, require confidence in the compilers/maintainers of the lists, and there is always the danger that a legitimate e-mail may be prevented from getting through.
- Whitelists and approved channels — These work in the opposite way, by only permitting e-mails that are from known sources or which are sent via approved channels. They rely on businesses maintaining the approved

lists and on their contacts having been informed of, and using, the correct channels. For many businesses these may be unduly restrictive.

- E-mail address concealment — Many companies are seeking to minimise the exposure of their e-mail addresses and those of their employees by, for example, swapping or inserting words such as 'REMOVE-THIS' within e-mail addresses posted on their websites to ensure they are not read correctly by parsing software, or by not posting e-mail addresses on their websites at all.
- Filtering — Filtering systems are becoming more sophisticated by, for example, singling out near identical messages sent to many recipients and by simply picking out e-mails containing particular keywords unlikely to appear in legitimate communications.

The costs of some these systems and practices to business can be prohibitive, however, and because they are seeking to treat the problem rather than prevent it, technical methods are unlikely ever to provide a complete solution.

Other new initiatives are being taken, however, which do seek to stop spam at its source. Many of these initiatives involve international cooperation. Within the EU, 13 countries have reached an agreement to share information and pursue complaints across their borders in a pan-EU drive to combat spam, the remaining member states are being encouraged to follow suit.²⁴ Since most of world's spam originates from outside the EU, it is to be welcomed that the EU has also united with Asia in its recent anti-spam drive. A joint statement of international cooperation on spam followed the Asia-Europe conference on e-commerce held in London on 21–22 February, 2005 which involved China

and South Korea — two of the world's five spam source countries which together account for around 22 per cent of the world's spam.²⁵ The USA, too, has been taking international non-legislative initiatives, with the FTC announcing an Action Plan on Spam Enforcement in which it joined forces with 19 enforcement agencies from 15 countries around the world in October 2004.²⁶

CONCLUSIONS

E-mail spamming is still a growing, global problem that faces both e-mail users and legitimate marketing businesses. The new laws operating in the EU and USA, are unlikely, as they stand, to rein in the small band of dedicated spammers who generate the majority of unwanted e-mail traffic. Likewise, the ever more sophisticated technical solutions to spam, whilst they may ease the effects of the problem, will probably never provide a complete solution. It is hoped, however, that these measures, combined with the trend of growing international cooperation between countries that include the world's principal sources of spam, will finally start to tackle the problem, and that the steps taken will start to have more of an effect on the spammers than on legitimate marketing companies.

© Bristows

References and Notes

- 1 See, for example, Commission press release dated 24 February 2005 entitled 'EU and Asia unite against "spam"'.
2 Anon (2005) 'New email scam promises money from the late Sir Dennis Thatcher's will, reports *Sophos*', *Sophos*, 16th March, 2005, available at www.sophos.com/spaminfo/articles.
3 The Privacy and Electronic Communications (EC Directive) Regulations 2003.
4 Nettleton, E. (2004) 'Electronic marketing and the new anti-spam regulations', *Journal of Database Marketing & Customer Strategy Management*, Vol. 11, No. 3, pp. 235–240.
5 Nettleton, E. and Pham, C. (2005) 'Telephone marketing out in the cold?', *Journal of Database*

- Marketing & Customer Strategy Management*, Vol. 12, No. 2, pp. 172–176.
- 6 These were reportedly sent by two lawyers in Arizona in 1994 (see 'Pest Control' by Daniel Eilon and James Watt, *Legal Week* (Global Edition), 29 July 2004).
 - 7 E.g. a spam e-mailer reportedly testified at the FTC Spam Forum that he could make a profit even if his response rate was less than 0.0001% (see the remarks of Timothy Muris at the Aspen Summit of 19 August 2003).
 - 8 Spamhaus 'SBL blocklist rationale', available at www.spamhaus.org/sbl/sbl-rationale.html.
 - 9 Anon (2005) 'New York man arrested in spam case, Sophos reports', *Sophos*, 18 February, available at www.sophos.com/spaminfo/articles.
 - 10 Anon (2004) 'The "dirty dozen" 2004: Sophos reveals the top spamming countries', *Sophos* 24 December, available at www.sophos.com/spaminfo/articles.
 - 11 The EU Commission's communication to the Council entitled 'European electronic communications regulation and markets 2004' (10th Report) and dated 2nd December, 2004, suggested that at the end of October 2004, although 20 member states had adopted the primary legislation required to implement the Directive, five member states (Belgium, the Czech Republic, Estonia, Greece and Luxembourg) had not. Substantive secondary legislation was also said to be outstanding.
 - 12 Closely followed by Spain, the UK and Germany (see Anon (2004) *op. cit.*)
 - 13 See EU Commission's communication *op. cit.*
 - 14 Nettleton, E. (2004) *op. cit.*
 - 15 Raw, H. (2004) 'Spam: Where's the beef?', *Computers & Law*, Vol. 15, No. 1, pp. 38–40.
 - 16 Spain, Denmark, Belgium, the Netherlands, Germany, Hungary, Poland, the Czech Republic, Slovakia and Slovenia have also adopted the opt-in regime (see the Commission's communication, *op. cit.*).
 - 17 Implementation in Italy was via the Personal Data Protection Code (legislative decree no. 196 dated 30 June, 2003) which supplemented earlier Italian legislation which already covered many of the principles of the Directive.
 - 18 Based on statements made by the Council in European Council (2004) 'Fight against "spam" — Council conclusions' section of press release, 9–10 December, 2004 (provisional version) following the 2629th Council meeting.
 - 19 For example, six such bills were introduced during the 106th Congress (1999–2000) including the first version of CAN-SPAM.
 - 20 Sullivan, J. and Leeuw, M. (2004) 'Opening up the CAN-SPAM Act', *Computers & Law*, Vol. 14, No. 6, pp. 17–20.
 - 21 For example, such links could be used by fraudsters as a well-disguised way of 'phishing'.
 - 22 This is also reportedly backed up by a suspended judgment for the total amount of the company's diet patch sales (US\$230,000). See FTC press release dated 31st March, 2005 entitled 'Diet patch sellers settle can-spam charges'.
 - 23 Details are provided on the FTC website: <http://www.ftc.gov/>.
 - 24 European Commission (2005) 'European countries launch joint drive to combat "spam"', Press Release, 7 February, 2005.
 - 25 Anon (2004) *op. cit.*
 - 26 Federal Trade Commission (2004) 'FTC, international agencies adopt action plan on spam enforcement', Press Release, 12th October.