

## Spam – the meat of the problem

Mike Butler, Hammonds

The current problem is as much about curbing the behaviour of a small but pervasive minority as it is about regulating the vast majority of existing users of email

The regulators have been busy again. As part of the European regulatory framework, Member States are required to implement the Directive on Privacy and Electronic Communications (“Privacy Directive”) by 31 October 2003. In the UK, the Department of Trade and Industry (DTI) has recently published draft legislation - the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the “Regulations”) - together with a consultation paper on the draft Regulations. The scope of Regulations has been dealt with elsewhere.<sup>1</sup> In broad terms, the Regulations regulate unsolicited email and short message services (SMS) (up to 160 characters in length), cookies, traffic and location data and subscriber entries. The purpose of this article is to look in more depth at two key issues: will the Regulations make a difference to unsolicited email and SMS and what are the compliance effects for legitimate businesses in view of the DTI’s guidance on the Privacy Directive?

### A. Scope of the problem

“Spam” is most succinctly defined as unsolicited bulk email. A more technical definition is that an electronic message is spam if:

- the recipient’s personal identity and context are irrelevant because the message is equally applicable to many other potential recipients;
- the recipient has not verifiably granted deliberate, explicit and still revocable permission for it to be sent; and
- the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

Spam therefore covers a multitude of types of electronic communication. But a differentiation needs to be made between legitimate unsolicited commercial email (“identified spam”) and illegitimate (or quasi-legitimate) unsolicited email (“junk spam”). Both are caught by the Privacy Directive and Regulations but it is the latter which is clogging up bandwidth and crashing systems.

Identified spam emanates from organisations we know. It may be a promotional email from an on-line retailer we have bought a book from or an

SMS from a newspaper where we entered a competition. In neither of these communications have we “verifiably granted deliberate, explicit” consent. However, we feel comfortable that any request we make to stop receiving these emails or SMS’s will be honoured as we are dealing with reputable, identifiable organisations.

Junk spam on the other hand comes from organisations we neither know nor want to know. Most often, it is not clear who sent the junk spam. Often the content of junk spam is

pornographic. Frequently, the email is misleading and, more often than not, fraudulent.

Note the following:

- Around two thirds of spam messages are deceptive or misleading, according to an April 2003 study by the Federal Trade Commission;
- A London-based anti-spam group has estimated that just 180 individuals are responsible for 90% of the spam in North America and Europe;
- There is pervasive use of remailers over the Internet where it is difficult (if not impossible) to identify the sender of the email;
- Recently, the Attorney General in the US brought charges against Howard Carmack (otherwise known as the “Buffalo Spammer”) for alleged identity theft and forgery that allowed him to send more than 825 million email messages through the ISP EarthLink.

The current problem is therefore as much about curbing the behaviour of a small but pervasive minority as it is about regulating the vast majority of existing users of email. Given that this minority is unlikely to be concerned with civil remedies, the problem cannot be addressed by regulation alone. As the Federal Trade Commission has recently said in the US there is no “silver bullet” but:

*Solving the problem of bulk unsolicited commercial emails will likely necessitate an integrated effort involving a variety of technological, legal and consumer action, rather than one single solution.*

Accordingly, it is worthwhile to look at how the US is approaching this issue before we consider the effect of the Privacy Directive and Regulations in the EU.

### **B. Spam USA**

---

So far 26 US states have passed anti-spam laws of one kind or another. Not all of them have been successful, and such are the differences in approach that staunch self-regulators like the Direct Marketing Association have called for legislation at a federal level. Nevada was the first state to pass an anti-spam bill back in 1997. This simply requires direct marketers to offer recipients the opportunity to be removed from email distribution lists. Washington State laws have had slightly more impact with several high profile anti-spam cases based on law that prohibits sending email to state residents that falsifies the sender or subject line. Some states, including California, require unsolicited email to be identified with “ADV” in the subject line and to carry clear opt-out instructions and contact information. The inclusion of ADV in a subject line allows filtering software to weed out incoming spam. Some of these states allow recipients of unlawful spam to sue for damages, although penalties against spam are relatively small. In the first successful claim under Kansas anti-spam legislation, the consumer was awarded \$500 by a small claims court. Critics of state law have suggested that the impact on spammers of state legislation has been minimal whilst leaving legitimate organisations, like credit card companies and distance sellers, increasingly confused.

### **C. Virginia**

---

Recent amendments to the Virginia Computer Crimes Act are therefore significant for two reasons. First, they contain anti-spam provisions which are more robust than most. Secondly, Virginia is the home state of several major internet service providers including America Online and it is estimated that around half of all internet traffic flows through the state. It is therefore suggested that the potential jurisdictional reach of the legislation is enormous both within and outside the US. Nevertheless, enforcement will always be a problem. Shane Ham, a senior analyst at the Progressive Policy Institute, a Democratic think tank, has been widely quoted as saying that he cannot imagine the state attorney general in

Virginia getting a lot of co-operation from California police when Virginia wants them to arrest and extradite someone wanted for spamming.

The new Virginia legislation provides criminal penalties for fraudulent, high volume spamming. It outlaws practices such as forging the return address line of an email or hacking a computer to send spam surreptitiously. Those found guilty of sending more than 10 000 defective emails within a 24 hour period or 100 000 in a 30 day period face one to five years imprisonment and forfeiture of profits and assets connected to spamming. Similar penalties apply to spammers who generate \$1 000 in revenue from a specific transmission, or \$50 000 from total transmissions. Prosecutors and the Attorney General will also be authorised to seize profits, computer equipment and all property connected with the offence. Theoretically, legitimate direct marketers who send out large mailings should not be concerned that they will accidentally fall foul of the legislation as it requires any altering of the email header or routing information to be done consciously with intent for the commission of an offence.

### **D. Federal law**

---

There is currently no anti-spam legislation at federal level, although the FTC has prosecuted a number of spammers using existing anti-fraud legislation and on its website encourages recipients to report spammers. Nevertheless, Congress, which has so far rejected proposals for federal anti-spam legislation, is now expected to give serious consideration to several new proposals. One of these is the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing) which is similar to the Virginia legislation. Another bill, proposed by New York Senator Charles Schumer, is perhaps too draconian. This would outlaw all spam, including non-fraudulent mailings. The bill, which has yet to be drawn up, would create a national registry or opt-out list with penalties for bulk emailers who do not weed out names on the registry database from their mailing list.

### **E. Effect of the regulations on spam**

---

The Privacy Directive is quite clear on spam. Article 13(1) states:

*The use of ... electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.*

The definition of “electronic mail” is widely drawn to mean any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient. Recital 40 specifically states that this definition includes SMS messages.

Simply put, the requirement is to obtain the consent of the subscriber. The exception to this requirement (known as “soft opt-in”) is contained in Article 13(2) which states:

*...where a natural or legal person obtains from its customers their electronic contact details for electronic mail, **in the context of a sale of the product or a service** ... the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use. (emphasis added)*

Again, this is quite clear. The exception to the requirement for consent is triggered only where the email address is obtained “in the context of the sale of a product or a service”. This is naturally circumscribed and does not, for example, include other legitimate means for obtaining email addresses such as registrations on websites or email addresses obtained in response to questionnaires.

However, the DTI has taken a more liberal approach to when the soft opt-in approach may be used. The equivalent requirement in the Regulations (regulation 21(3)(a)) states that:

*... [the sender] has obtained the contact details of the recipient of that electronic mail in the course of the sale **or negotiations** for the sale of a product or service to that recipient.*

Not content with the addition of the words “or negotiations” (going beyond the wording in the Privacy Directive), the DTI has indicated in its consultation paper that it will not be concerned with looking at the precise details of how the

email address was obtained provided it was obtained “legitimately” in the broadest sense of the word. The DTI asks:

*...should customer relationship for these purposes be confined to situations only where the email addressee has previously bought something or should it apply to prospective customers as well (e.g. where someone has registered an interest in a product and allowed their email to be recorded for future marketing use but under an opt-out rather than opt-in process)?*

*Our view is that the most important safeguards here are that contact details are fairly collected and subscribers are clearly informed of, and given a chance to object to, use of their data for direct marketing by that same business. As long as these conditions are met, and there is a direct relationship of some kind between the two parties, it does not seem necessary to insist that there must have been an actual purchase for this exemption to apply.*

Similarly, the DTI is looking to adopt a common sense approach to the “similar products” rule. In its consultation paper, it states that businesses will be able to market the kind of products the addressee would have “reasonably expected it to market at the time they gave or agreed to use of their contact details”. Indeed, the DTI goes on to state that it is sensible to give a “broader” rather than a narrower interpretation to the similar products restriction.

## F. Compliance concerns

The result of the DTI’s approach may mean that businesses have fewer compliance concerns than at first envisaged. In effect, the broadening of the soft opt-in approach to legitimate collection of email addresses will mean that businesses may choose to continue existing practices. For example, where email addresses are collected from websites (e.g. in response to questionnaires or entries into competitions or from registration), then businesses may choose to continue to use an opt-out approach and seek to rely on the broad interpretation of the soft opt-in regime favoured by the DTI.

A more difficult point relates to the issue of what exactly is required by “consent”. In practical terms, it is not always easy to say when electronic consent has been obtained. For example, is a box

*It is not always easy to say when electronic consent has been obtained*

which is already ticked next to the words “I consent to receiving marketing information from you” valid consent? It would certainly seem to go against the spirit of the Privacy Directive (in particular, recital 40 refers to the “explicit consent” being obtained before direct marketing communications are sent). Similarly, the British Codes of Advertising specify a regime very similar to the Privacy Directive and require “explicit consent” to direct marketing provided that businesses may market similar products to their “existing customers” without explicit consent. Further guidance from the DTI will be required on this issue.

### G. Enforcement and criminal remedies

---

As noted above, a number of states in the US have sought to criminalise certain types of spamming and law enforcement agencies have actively targeted the fraudulent use of spam (e.g. the Buffalo Spammer). In comparison, the Privacy Directive and Regulations are toothless as against the use of junk spam. In the UK, the enforcement powers for the Regulations will be those available to the Information Commissioner under the Data Protection Act 1998. This will involve the use of enforcement notices requiring remedial action to be taken. In the face of the senders of junk spam, such actions will be too little and too late.

Nor do existing European proposals to combat criminal activity against information systems adequately address the problem. In February 2003, the European Commission adopted a proposal for a Council Framework Decision on attacks against information systems. The draft Decision requires Member States to implement a new offence to cover “illegal interference”. This offence will cover the intentional and serious hindering or interruption without permission of the functioning of an information system; i.e. it will criminalise “denial of service attacks” as well as deliberate spreading of viruses.

The draft Decision does not address the issues currently faced by the growth of junk spam. In particular, malicious misrepresentation (“spoofing”) is excluded from the scope of the Decision. Accordingly, both for the present and

future, there will be inadequate protection against the real problem of junk spam.

### H. Conclusion

---

The compliance consequences of the Regulations may not be as great as originally contemplated. In particular, the liberal interpretation of the soft opt-in exemption by the DTI may allow many organisations to continue with their existing practices for the collection and use of email addresses.

Neither the Privacy Directive nor the Regulations adequately addresses the issue of junk spam. This issue will only be properly addressed through appropriate criminal legislation, co-operation of law enforcement agencies and efforts made by service providers (see further below). The Privacy Directive is no silver bullet. “Janita” will still appear in your inbox inviting you to view her through a web-cam and offers of low-price cosmetic surgery will continue to pour in. Meanwhile, legitimate businesses will be concerned to deal with their own compliance whilst wrestling with the issues of consent and communications with existing customers.

The co-operation of service providers will be vital to the effectiveness of preventing junk spam. AOL, Microsoft and Yahoo! announced collectively at the end of April their commitment to work together and to continue to work actively with law enforcement agencies in the US to fight spam. In particular, they aim to develop better mechanisms for preserving electronic evidence relating to spamming activities and to co-ordinate ISP and industry enforcement efforts generally in the referral of spammers for enforcement action by the police and government agencies. It can only be hoped that the EU enforcement agencies and legislators concentrate their efforts on where the real problem lies rather than seeking to put yet more red tape in the way of legitimate businesses.

Mike Butler, Solicitor, Hammonds

Michael.Butler@hammonds.com

### FOOTNOTES

---

<sup>1</sup> See article by Mark Crichard in [2003] 19 CLSR 299