

Evidence to APIG Enquiry into Unsolicited Bulk Email
By: The Internet Policy Agency, 27th June 2003

1 What is the legal position?

1.1) The techniques used by many spammers involve hacking¹ and identity theft activities which are often illegal in the sender's country. They may also be infringing various specific vertical legislation regarding the advertising or sale of prohibited products, or the use of pyramid marketing.

1.2) The sending of UBE in Europe is governed by the provisions of the main Data Protection Directive² 95/46/EC transposed as the Data Protection Act 1998³:

- The Office of the Information Commissioner has confirmed⁴ that Email addresses are Personal Data "In the context of the Internet, many e-mail addresses are personal data where the e-mail address clearly identifies a particular individual."
- As described in Opinion 1/2000 of the Article 29 Data Protection Working Party⁵, in particular:
 - Where email addresses are collected directly from a person, they must be informed of the purposes at the time of collection (Article 10).
 - The data subject must be allowed to object at the time of collection, of subsequent use, or when the list is resold (Article 14)
 - Where the email address is collected from a public space (eg website or usenet) on the Internet, it is unfair processing (Article 6(1)(a)), contrary to the purpose principle (Article 6(1)(b)), and does not satisfy the balance of interest test (Article 7(f)).

1.3) It is contrary to the provisions of Article 10 of the Distance Selling Directive⁶ 97/7/EC:

- "individual communications may be used only where there is no clear objection from the consumer". (Which can only realistically be given by opting in.)
- This article was not transposed into the UK's Consumer Protection (Distance Selling) Regulations 2000⁷ as it was felt that the combination of the Data Protection Act 1998 and Industry Self Regulation were already a sufficient safeguard.

1.4) Most UBE, even that sent by organisations which otherwise regard themselves as acting within the law, fail to abide by Article 7 of the Electronic Commerce Directive⁸ 2000/31/EC, transposed as the Electronic Commerce (EC Directive) Regulations 2002⁹:

- UBE must be "identifiable clearly and unambiguously as soon as it is received". (For example, by the use of an ADV: prefix on the title.)

1.5) The Directive on privacy and electronic communications¹⁰ 2002/58/EC, to be transposed as the [Draft] Privacy and Electronic Communications (EC Directive) Regulations 2003¹¹ will introduce a "soft-opt-in" scheme from November 2003.

2 Further Considerations

2.1) Some provisions in the Directives above only apply to natural (rather than legal) persons. However, if an email that would only be of interest to a natural person (for example, an invitation to buy Viagra sent to the sales address of a shipping company), is sent to the address of a legal person, then it ought to be construed that a natural person is the intended recipient, and the full protection of the Directives should be provided.

2.2) UBE that complies with the Directives above may still be considered unacceptable according to the Acceptable Use Policy of individual ISPs, which in particular would make no distinction between emails sent to individual or corporate email addresses (natural/legal persons).

¹ Including the placing of Viruses and Trojans.

² http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

³ <http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

⁴ 1998 Legal Guidance para 2.3.3

⁵ http://europa.eu.int/comm/internal_market/privacy/workinggroup_en.htm

⁶ http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0007&model=guichett

⁷ <http://www.hmso.gov.uk/si/si2000/20002334.htm>

⁸ http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

⁹ <http://www.hmso.gov.uk/si/si2002/20022013.htm>

¹⁰ http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

¹¹ http://www.dti.gov.uk/industries/ecomunications/directive_on_privacy_electronic_communications_200258ec.html

Appendix – Background Information

A1 What is Spam¹²?

A1.1) "Spam" is a nickname for Unsolicited Bulk Email (UBE), sometimes called "junk email". It is a widespread problem on the Internet because of the volumes involved and the indiscriminate nature of its sending. There can be few email users who do not have first hand experience of receiving UBE, often in significant quantity.

A1.2) Spam is carried by the normal email service offered to customers of ISPs. Being an international problem, legislation in individual countries cannot alone stop the delivery of Spam, but it sets a political context which increasingly marginalizes its production.

A2 What is not Spam?

A2.1) Email is not only a means of person to person communication, but also a powerful and cost effective business tool. Some ISPs have historically resisted the regulation of UBE thinking that it will restrict their ability to serve the legitimate market for opted-in marketing materials.

A2.2) The recent passage of the EU's Directive on privacy and electronic communications should allow the UK to establish sensible rules for legitimate opt-in mailings and agree to concentrate on widely agreed measures to combat unwanted Spam.

A3 Why is Spam unacceptable?

The sending of UBE is considered to be unacceptable behaviour because

- It interferes with the operation of the Internet.
- It creates unwanted, distracting, time-consuming and potentially distressing traffic for the recipients.
- It creates support overheads for ISPs who must deal not only with the complaints from their own customers who have received unwanted email, but also with the reports submitted by others, demanding action when their own customers have sent the UBE.
- In its commercial form UBE usually promotes goods of dubious provenance, legality or taste.

A4 Why do people send Spam?

People sending UBE have several motives.

- Some are trying to generate traffic to websites, which may in turn create sales or banner advertising revenue for those websites, or are used to gather credit card or other financial details which are then abused or used for identity theft.
- Others are promoting well known pyramid marketing schemes and financial scams.
- Members of the public are unlikely to complain if ripped off by a website selling illegal products, or where it is embarrassing to admit having attempted to buy.
- A proportion (more susceptible to local regulation than those above) is sent by "clueless newbies" who have often been sold illegally gathered lists of email addresses allegedly interested in their direct mail products, business services and political causes.

A5 Why do people receive Spam?

Most UBE is truly indiscriminate. It is not targeted in any way. The addresses to which it is sent are normally derived from lists compiled from earlier lists. Addresses are added to these lists because the email address has been:

- harvested from a web page or other public source
- generated automatically by a system which guesses email addresses.
- gathered from an organisation that has been previously emailed.
- included in a request to be removed from a previous UBE list.

¹² SPAM is a Registered Trademark of Hormel Foods Inc who have been manufacturing SPAM Luncheon Meat since the 1930s. They explain the legal complexities which occur when a trademark becomes a slang term at http://www.spam.com/ci/ci_in.htm

Evidence to APIG Enquiry into Unsolicited Bulk Email
By: The Internet Policy Agency, 27th June 2003

A6 Does it cause particular harm to children?

A6.1) UBE is unlikely to be intended to harm children, but because it is indiscriminate, email accounts belonging to children will receive email promoting adult or other unsuitable products.

A6.2) Some UBE appears to promote pictures of child abuse.

- Such UBE can be investigated by the Internet Watch Foundation through their reporting mechanism at <http://www.iwf.org.uk> .
- In the year to April 2002, only 11 website takedown notices issued by the IWF (1% of the total) were as a result of reports of Spam, although those reports were 17% of the total.

A6.3) It is also important to realise that in order to make their emails more attractive, the senders will often lie about the recipient having requested the email in a previous conversation, or by subscribing to a website. However, do not assume that children have done this, simply because an email says so.

A7 What can be done about Spam?

A7.1) The vast majority of the emails originate overseas, and the perpetrators are therefore difficult to prosecute. In order to obscure their identity, in many cases they hack into vulnerable computers and the emails appear to be sent from these compromised machines.

A7.2) Internet Service Providers (for whom Spam disrupts the smooth operation of the Internet) co-operate to reduce the number of computers (most of which belong to their customers) which are vulnerable in this way, and to trace and remove the accounts from Spammers¹³.

A7.3) Most email addresses used by Spammers have been obtained from third parties, so be very careful when using your email address when online. In particular, users should never respond to "unsubscribe" requests contained in unsolicited emails they receive, as this will confirm the validity of the email address. This advice is somewhat at odds with the provisions of the draft Privacy and Electronic Communications Regulations¹⁴, which require "a simple means ... of refusing the use of his contact details ... at the time of each subsequent communication".

A7.4) Filtering, to remove emails with spam-like content can appear attractive,

- but the widespread use of filtering has already caused spam to evolve, making it more difficult to detect.
- there is a risk of "false positives" – wanted emails that are branded as spam and in some circumstances incorrectly discarded.
- one manifestation of this has been called the "Scunthorpe effect".
- at the time of writing, solicited responses from bona-fide ecommerce sites seem particularly prone to false positives.

¹³ Industry Best Practice is described in a LINX document: <http://www.linx.net/noncore/bcp/ube-bcp.html>

¹⁴ http://www.dti.gov.uk/industry_files/word/annex_2.doc