

Is the Content of Spam Illegal?

1 Introduction

The E-Privacy Directive prohibits the sending of unsolicited marketing emails to individuals within the European Union. The only exception is where there is an existing business relationship and the email advertises similar goods or services to those already supplied. In the UK, the provisions of the Directive were brought into force in December 2003. However, it is clear that unsolicited email will continue to arrive from outside Europe, and of course not everyone in Europe can be expected to obey the new law immediately.

Unsolicited email is often called “spam”, though some reserve the term for particular types of email, which they often characterise as the promotion of illegal material in an illegal manner. This document examines the narrow issue as to what extent the *content* of an email can be illegal within the UK.

In Section 2 we review the general legislative framework relating to email, in Section 3 we consider some technical issues that arise with the structure of emails and then in Section 4 we address some generic legislative issues. Becoming more specific, Section 5 then makes clear that the content of some “spam” is illegal and the senders can be committing serious criminal offences. Other message content is illegal, but at a lower level of criminality.

Please note that this document should not be read as or understood to be legal advice. It surveys a complex area and individual messages may exhibit features that override the necessarily general observations made here.

2 Generic Legislation

2.1 Communications Act

The Communications Act 2003 makes it an offence, as did the Telecommunications Act 1984 before it, to send or cause to be sent “by means of a public electronic communications network” a “message or other matter that is grossly offensive or of an indecent, obscene or menacing character” (s127).

2.2 E-Commerce Legislation

The “E-Commerce Directive” 2000/31/EC has been transcribed into UK law as “The Electronic Commerce (EC Directive) Regulations 2002”, SI 2002/2013. The regulations require unsolicited commercial email to be clearly marked as such when received. The content must also be clearly identifiable as a commercial communication and must identify the person on whose behalf it is made.

The directive also gives specific immunities to Information Society Providers (such as ISPs). These immunities relate to “cacheing”, “hosting” and “mere conduit”. In

practice these mean that where an ISP is merely delivering email then they will have committed no offence, whatever the content of that email.

An agency that sent email on behalf of clients is unlikely to be sheltered by these immunities. The UK regulations specify that the limitations on liability of intermediaries for “mere conduit” apply only where the service provider does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained.

2.3 Distance Selling Legislation

The “Distance Selling Directive” 97/7/EC has been transcribed into UK law as “The Consumer Protection (Distance Selling) Regulations”, SI 2000/2334. It places various burdens onto those who make contact with consumers in order to sell things to them. Should they fail to meet various requirements then they may be unable to enforce contracts and may be required to take back rejected goods. However, failure to meet these requirements does not make the content of any email illegal per se.

2.4 E-Privacy Legislation

The “Directive on privacy and electronic communications” 2002/58/EC has been transcribed into UK law as “The Privacy and Electronic Communications (EC Directive) Regulations”, SI2003/2426. It brings in a “soft opt-in” regime for direct marketing email. It also prohibits the disguising or concealing of the sender.

The regulations apply to anyone who “sends or instigates the sending” of email or “permits their line to be used” to send email in breach of the consent rules. This is intended to allow some latitude in the taking action against agents as well as the person whose goods/services are being promoted where there’s a degree of shared responsibility.

3 Technical Issues Relating to Email

3.1 Attachments

Email often appears to contain pictures, however on close inspection it can be seen that the email only contained code (specific forms of URL or scripting) that caused the pictures to be fetched. Whether you can see the pictures will depend upon the capabilities (and configuration) of your email client.

In *R v Waddon* 1999, the court held that publishing an article under s1(3)(b) of the Obscene Publications Act 1959 included data stored electronically and transmitted. To transmit meant simply to send on from one place or person to another. So the court is likely to look at the intent of the sender (viz that the picture might be expected to be displayed) rather than a narrow technical claim that it might not have been displayed in all cases. Note that the *R v Graham Westgarth Smith* 2002 appeal decision established that there is no offence committed by the receiver if a picture does appear, provided that the recipient is unaware that the email contains or is likely to contain an indecent image.

3.2 Links Generally

Emails often contain links to material which when clicked upon will cause the recipient's browser to display what was linked to. Again the innocent receiver is protected where the link appears innocuous, but *R v Jayson 2002* held that the voluntary downloading of an indecent image of a child to a computer screen was the illegal act of "making".

There has been no specific UK case law relating to links, though there have been a number of cases decided elsewhere relating to links between websites (especially, so-called "deep links" into the heart of competitor's websites). No real pattern has yet emerged. There is one relevant case in defamation law (*Hird v Wood 1894*) where a court held that the defendant had defamed the plaintiff by merely standing on a road and mutely pointing out a path which, if followed, allowed one to view a notice on which a defamatory statement had been written.

The police and the IWF have generally taken the view that web pages containing links to illegal material are "advertising" (because the Protection of Children Act 1978 mentions this specifically) and proceeded on that basis. This seems an appropriate way of viewing links within email, where the whole email is likely to be "advertising" anyway. This approach of looking at the intent of providing the links has the advantage of not catching someone whose links were to innocuous material originally, but the remote site has changed content (and often ownership) in the meantime.

3.3 "Bugs"

Links can sometimes be customised on a per email basis. This means that the owner of a website will be able to determine precisely which recipient clicked on a link or, where pictures were automatically fetched, which recipients just opened the email. There does not appear to be any requirement to inform the recipient of this happening, though of course the logs created at the website (or picture server) would be subject to Data Protection legislation if such legislation exists in the sender's jurisdiction.

The E-Privacy Regulations do contain provisions relating to "cookies" and similar Internet tracking devices. However, for these to apply there must be some data storage on the user's machine.

4 Generic Legislative Issues

4.1 Email Sent to Children

There are some specific offences that can be committed by sending material to children that would not be committed if it was sent to an adult. For example, the Obscene Publications Act 1959, prohibits the publication of material likely to corrupt and deprave persons likely in all the circumstances to see hear or read it. Some spam does fall into this category, so a spammer could fall foul of this provision even if they were not specifically targeting children, though complex issues of intent (*mens rea*) would arise. This has not been tested with regard to email, but the OPA was successfully used against a website operator *R v Perrin 2002*, which was tested at

appeal, though it is not believed that the possibility of children seeing the material concerned was specifically referred to.

It will also be an offence under s12 of the Sexual Offences Act 2003 to cause a child to watch a sexual act (including showing an image of such an act) for the purpose of sexual gratification. However, this is unlikely to catch a spammer unless their email was clearly targeting children.

4.2 Viruses, Worms etc

Anyone who creates or distributes a virus or other “malware” is likely to have committed an offence under s3 of the Computer Misuse Act 1990. However, if someone’s computer becomes infected by such a virus without their knowledge then the mens rea test in s3(1) would not be met and they will not have committed an offence. Once someone has been informed that their machine has been infected, then they will meet the test of s3(1), but they may not meet the test of “intent” in s3(2) even if they are reckless in failing to act to remove the malware.

4.3 Tax Laws

Different jurisdictions have different tax laws and different consumer protection legislation as to how the true costs of products should be displayed. In the UK bodies such as Trading Standards and the Advertising Standards Authority (ASA) require that goods advertised by VAT registered traders to consumers must show VAT inclusive prices. Also, the E-Commerce regulations require online service providers to make it clear whether any prices quoted do or do not include taxes and delivery costs.

4.4 Misleading Advertisements

Many spam emails make remarkable claims for products, one currently thinks of those that will enhance various private body parts. The products themselves are generally legal, but making false claims about them is not.

The Control of Misleading Advertisements Regulations are handled by the Advertising Standards Authority (ASA) and the Trading Standards service. Agencies such as the Financial Services Authority and the Medicines Control Agency handle more specialised advertising complaints. The Office of Fair Trading has an oversight role, but usually only steps in when other agencies have been unable to deal adequately with a complaint.

5 Specific Legislative Issues

This section considers particular types of products or services that are regularly promoted by unsolicited email.

5.1 Child Pornography

Indecent images of children are covered by the Protection of Children Act 1978 as amended several times, most recently by the Sexual Offences Act 2003. In particular,

the Act makes advertising such material illegal. Hence the sender of email that purports to offer such material – even if the claim turns out to be false – has committed a serious offence.

5.2 Adult Pornography

The relevant legislation is the Obscene Publications Act 1959, which in s1(1) sets out the test for obscenity: “For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.”

We have already discussed the issues of including obscene material within an email or linking to it. The law also makes it illegal to advertise obscene material “for sale or for letting on hire”. So if a spam email was advertising material that was obscene under the OPA then it would be illegal.

5.3 Medicines etc

All advertising for medicines in the UK is subject to the requirements of the Medicines (Advertising) Regulations 1994 (SI 1994/1932 as amended). These regulations implement European Directive 92/29/EC, codified as Title VIII of Directive 2001/83/EC. The regulations apply both to advertising for any medicines to health professionals and to advertising to the public for medicines available “over the counter”. The promotion to the public of medicines, such as ‘Viagra’, that are available only on prescription, is prohibited.

Slimming products may be legally advertised. However there are detailed rules in the ASA “Cap Code”. As with all health and beauty advertising, advertisers must hold rigorous scientific evidence to show that their products work as claimed: testimonials alone are not enough. They should be careful to ensure that the name of the product does not include an implied claim that they cannot support, e.g. Fatloss, they should not suggest that their product will not fail and, if they have proved that their product works, they cannot claim that normally overweight individuals will lose more than 2lbs a week. Where these rules are not followed, the ASA can refer the matter to the Office of Fair Trading for enforcement action.

5.4 ...and many, many more

There are any number of products and services that regularly appear in spam and are subject to specific legislation. The Financial Services Authority strictly regulates the selling of financial products and there are a number of specific regulations relating to the E-Commerce Directive. The Tobacco Advertising and Promotion Act 2002 bans tobacco adverts. Satellite/Cable Piracy devices are illegal to sell and illegal to advertise. “Advanced Fee Fraud” emails (sometime called “419 scams” or “Nigerian Letters”) are attempted fraud and hence illegal. Even fake University Diplomas (for UK institutions) are made illegal by s214 of the Education Reform Act 1988.

However, with the caveats already noted about misleading advertisements and the general rules about unsolicited email, there will be nothing illegal about the *content* of emails advertising such things as “home working”, dating agencies, laser printer toner cartridges, cheap watches, coffee makers, chocolates or even Valentine’s Day flowers.

6 Summary

Leaving aside the issues of when direct marketing email is permitted, some specific content, notably pornography, adverts for prescription medicines and many financial products is illegal within the UK. However, many products are not of themselves illegal and so it is incorrect, to always equate “unwanted junk email” with “illegal products advertised illegally”.

Selected Bibliography & Links

Computer Misuse Act 1990

http://www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Communications Act 2003

<http://www.legislation.hmso.gov.uk/acts/acts2003/20030021.htm>

Sexual Offences Act 2003

<http://www.legislation.hmso.gov.uk/acts/acts2003/20030042.htm>

The Electronic Commerce (EC Directive) Regulations 2002

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

The Consumer Protection (Distance Selling) Regulations 2000

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

The Privacy and Electronic Communications (EC Directive) Regulations 2003

<http://www.hmso.gov.uk/si/si2003/20032426.htm>

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (known as the Distance Selling Directive)

[http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!
CELEXnumdoc&numdoc=31997L0007](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31997L0007)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

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

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

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

Advertising Standards Authority

<http://www.asa.org.uk/>

The British Code of Advertising, Sales Promotion & Direct Marketing (the CAP code)

http://www.asa.org.uk/the_codes/

Department of Trade and Industry

E-Commerce generally

<http://www.dti.gov.uk/ccp/topics1/ecommm.htm>

Implementation of the E-Commerce Directive

http://www.dti.gov.uk/industries/ecommunications/electronic_commerce_directive_0031ec.html

E-Privacy Directive

http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html

Financial Services Authority

<http://www.fsa.gov.uk/>

HM Treasury

http://www.hm-treasury.gov.uk/Documents/Financial_Services/Regulating_Financial_Services/fin_rsf_edirec.cfm

Medicines Control Agency

<http://www.mca.gov.uk/ourwork/advertpromed/regprommed.htm>

Metropolitan Police Fraud Alert Site

<http://www.met.police.uk/fraudalert>

Office of Fair Trading

<http://www.offt.gov.uk>

Trading Standards

<http://www.tradingstandards.gov.uk/>