

## Understanding the law with respect to marketing by email

*By Dr C. N. M. Pounder, Amberhawk Training Limited*

*Dr Chris Pounder has worked in the field of data protection for over 30 years. Currently he is a Director of Amberhawk Training Limited which provides advanced training in data protection, freedom of information, information security (e.g. ISEB) and other aspects information law. The article is based on that published in the **Journal of Database Marketing & Customer Strategy Management** (14 November 2011). The article has been modified in order to help ISEB delegates understand the marketing rules for the Data Protection qualification as they apply to electronic mail.*

### Introduction

The Information Commissioner has recently published a “Guide to the Privacy and Electronic Communications Regulations” (the “Guide”); this article reviews some of the content of this guidance in the context of email marketing. Readers working for organisations that employ behavioural advertising techniques, telephone marketing, fax marketing, drop cookies with respect to web-site navigation or provide any service via the Internet are well advised to look at this Guide in the context of their operations.

The reason: as the new powers associated with the Privacy and Electronic Communications Regulations (PECR) enable the Information Commissioner to impose civil monetary penalties of up to £500,000 for serious breaches of the marketing rules, not to take notice of the new legal obligations carries a considerable risk.

### What is marketing?

Section 11 of the Data Protection Act 1998 refers to direct marketing as “the communication (by whatever means) of any **advertising** or **marketing** material which is directed to particular individuals”. Note that section 11 refers to the two concepts highlighted in bold; these go far wider than what one normally thinks of direct marketing (e.g. a mailing comprising a form which invites the data subject to apply for a loan).

It is the existence of these two terms which explains why the Commissioner states that “direct marketing as covering a wide range of activities that apply not just to the offer for sale of goods or services, but also to the promotion of an organisation’s aims and ideals”. So for example, “direct marketing” includes activities where a charity or a political party appealing for funds or support, an

# UNDERSTANDING THE LAW WITH RESPECT TO MARKETING BY EMAIL (Data Protection plus Privacy and Electronic Communications)



organisation that is encouraging individuals to write to their MP about something or to attend a public meeting or rally. This view was upheld by the Information Tribunal ruling which dismissed an appeal by the Scottish National Party that political campaigns were not covered by PECR (see references for Tribunal link).

Note the loosely worded “right to object to marketing” should really be expressed as the “right to object to the processing of personal data for a direct marketing purpose” as the section 11 right needs personal data to be processed. The right cannot apply to forms of marketing that do not need personal data to be processed (e.g. the familiar “dead letter” drop which invites you to order a take-away food from a local eatery).

### PECR adds to the Data Protection Act marketing obligations

Absent from the Guide is a reminder that an email address is most likely to constitute personal data as the data contains an identifiable name and the employer of a sender (e.g. [chris.pounder@amberhawk.com](mailto:chris.pounder@amberhawk.com)). Some email addresses might be of a very confidential nature depending on the employer (e.g. [fred.bloggs@huntingdon\\_life\\_sciences.com](mailto:fred.bloggs@huntingdon_life_sciences.com)) or if the individual has some kind of risk status (e.g. email addresses of individuals in witness protection).

Where email addresses are personal data, the Data Protection Act applies. In relation to direct marketing, the **main data protection rules** can be summarised thus:

- when email addresses are collected and **before** they are collected, the identity of the organisation wanting to use the email address and the marketing purpose must be identified to each individual who provides their email address. Such information, or privacy notice, has to be prominent and clear in meaning (e.g. not buried in the text of a web-form or couched in obscure language);
- any third-party marketing (e.g. where an organisation lets other companies use its email lists for their marketing purposes) needs the **prior consent** of the individual concerned; such **consent** has to be the fully informed, freely given, and include an indication of the individual’s wishes. In other words, an individual has to do something (e.g. click the send button). Doing nothing is not consent (e.g. if you don’t click this box, we will assume you have consented to the third party marketing);
- each mode of marketing should be identified (e.g. marketing by email) and either an “opt-out” (e.g. please tick the box if you don’t want marketing) or “opt-in” provided (e.g. please tick the

box if you want marketing). As we shall see with all electronic forms of marketing, PECR and the Guide pushes this “opt-in” or “opt-out” choice towards an individual’s positive decision to receive marketing (e.g. towards “opt-in”);

- if an individual objects to the use of his email address for a marketing purpose, then that objection prevails. There should be no more marketing emails sent to that individual unless that individual consents again (and arguably, all other forms of marketing that use personal data should also cease);
- all other data protection principles apply (e.g. email addresses should be kept up to date, secure and deleted when not needed). Note: I do not address these other Principles here

In addition, the Advertising Standard “UK Code of Non-broadcast Advertising, Sales Promotions and Direct Marketing” applies to the use of emails for a marketing purpose. Of particular relevance to most readers in the commercial sector will be Sections 8 to 10 (on sales promotions, distance selling and database practice).

When the above rules have been considered, **then** comes PECR’s additional rules associated with electronic mail.

### What is electronic mail?

The first important comment to make is that “electronic mail” is not limited to email. “Electronic mail” is defined as ‘any text, voice, sound, or image message sent over a public electronic communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient and includes messages sent using a short message service’.

In other words, email, text, picture and video marketing messages are all considered to be ‘electronic mail’. The Guide also considers the electronic marketing rule also applies to voicemail and answerphone messages left by marketers making marketing calls that would otherwise be ‘live’.

### What is the electronic mail marketing rule in PECR?

In summary, PECR generally requires an electronic mail marketer not to send **unsolicited** marketing material by electronic mail to an **individual subscriber** unless they have previously notified the sender that they have **consented** to receiving such communications. Note that I have highlighted

three important definitions here; it is important to know what they mean - we have already met **consent** (see third party marketing under “*PECR adds to Data Protection Act marketing obligations*”).

The first definition of importance is “**individual subscriber**” – this is the individual who pays the subscription. Note that this means that corporate subscribers are not protected by this rule, nor are users of a corporate subscription or of an individual’s subscription. For instance, suppose you pay for broadband internet at home and are allowed to set up several email addresses. Most likely, you would have distributed these email addresses to the rest of your family. In this example, you are the individual subscriber and your family members are users.

Now here is the subtle bit. Because users associated with an individual subscriber can’t easily be identified, a list that contains a **mixture** of users and individual subscribers will have to be treated as if it were a list of **all** individual subscribers. In this way, users of an individual subscription gain some of the protection afforded to the individual subscriber (in an indirect but unenforceable manner). Note that users of a corporate subscription will not get that protection (as is explained next).

For instance, suppose the Bloggs Family have a subscription to “*btinternet.com*”. The family’s email addresses are distributed to: [a.bloggs@btinternet.com](mailto:a.bloggs@btinternet.com), [b.bloggs@btinternet.com](mailto:b.bloggs@btinternet.com) and [c.bloggs@btinternet.com](mailto:c.bloggs@btinternet.com). If two of these individuals are users – can you identify the subscriber? Of course you can’t. So if a marketing person compiles a list of domestic email addresses, and sends an unsolicited email to everyone on that list, because he does not know which addresses are individual subscribers, he is therefore taking a risk:– a £500,000 one.

This is not the case for users associated with a corporate subscriber, as such users are easily identified (e.g. [chris.pounder@amberhawk.com](mailto:chris.pounder@amberhawk.com), [angela.bloggs@amberhawk.com](mailto:angela.bloggs@amberhawk.com)) from the domain name. In such circumstances, users of a corporate subscription have to rely on the protection afforded by the Data Protection Act and the right to object to marketing under the Data Protection Act (see above).

The next definition is “**unsolicited**”. Its meaning is determined through a definition of “**solicited**” so that an “**unsolicited**” marketing email is an email that is not **solicited**. The Guide defines a “**solicited**” message as “one that an individual subscriber has **opted into** receiving. It includes those messages that have not invited, but that for the time being they do not object to receiving”. Obviously, this includes all “opt-in” arrangements where the individual subscriber positively indicates that he wants to be marketed by email.

But what happens if an individual subscriber does not tick an “opt-out” box on a form (e.g. if you do not want to be contacted for a marketing purpose by email, please tick the box). Does this mean any

marketing email is solicited or unsolicited? Well this depends on who is doing the email marketing and the products being offered! As we shall see, not “solicited” (where solicited is defined by the Commissioner) is not the same thing as “unsolicited” and “not unsolicited” does not mean “solicited” (much to the confusion ISEB delegates!).

#### The soft opt-in.

The only exception to the **unsolicited** marketing rule is widely referred to as the “soft opt in” and the Guide explicitly defines the circumstances when an organisation may send marketing emails to an individual subscriber without an “opt-in”.

These circumstances are:

- the organisation has obtained the email address of an individual in the course of a sale or negotiations for the sale of a product or service to that individual;
- the marketing email only relates to material that describes the organisation’s similar products and services;
- each individual providing his email address is given a simple means of refusing (free of charge except for the cost of transmission) the use of the email address for marketing purposes; and
- when the email address was initially collected the individual did not refuse the use of those details for a email marketing purpose (see the data protection elements above if the email is personal data).

If these criteria cannot be satisfied, an organisation has to obtain the prior consent of each individual subscriber. For example, if the organisation wanted to send emails that promoted the products of another company in the same group, or if customers are asked to provide the email addresses of their friends for a marketing list. Obviously, if the individual subscriber objects to the email marketing, then any further marketing communication by email will be **unsolicited**.

#### Rules that apply to all marketing emails

There are two other rules associated with **any** email marketing that are worth mentioning.

- the identity of the sending organisation cannot be disguised or concealed in the marketing email;
- the sending organisation has not provided a valid address to which the recipient can send an opt-out request (e.g. an unsubscribe facility).

If email addresses are supplied to an organisation by a list provider, that organisation should obtain a warranty from the provider that states that the PECR and data protection rules have been applied

so that any marketing is lawful. Obviously, this and any indemnity guarantees should form part of a formal contract with the supplier and the list should be cleaned, prior to use, to remove those addresses where the individual subscriber has objected.

Finally, the new powers enable the Information Commissioner to impose civil monetary penalties of up to £500,000 for serious breaches of the above rules. So it really is a case of “UK spammers beware”.

#### Will PECR reduce spam?

This is the big question and the answer is sadly “no”. The PECR Regulations only apply to the UK – they do not apply to spam emails which are usually sent from abroad. However, having said that there is cause for limited optimism. Firstly, all Member States of the European Union have adopted more or less the same set of rules as in PECR:– probably in a more protective form than in the UK. So any spam from European mainland should be subject to the same rules as identified above and enforced by a national regulator – usually the national data protection authority.

With respect to marketing emails from non-EU countries there is a trend that such countries adopt a variant of the marketing rules already adopted by EU; however, this does not yet apply to every country. So don’t sell those shares in spam filter software providers yet. However, if your organisation does email marketing into Europe, or you are based in the UK, you MUST look at these rules or the national equivalent.

ENDS

Dr C N M Pounder  
December 2011

#### References:

1. Scottish National Party v The Information Commissioner, EA/2005/0021, 15th May 2006 <http://www.informationtribunal.gov.uk/DBFiles/Decision/i111/SNP.pdf>
2. Guide to the Privacy and Electronic Communications Regulations [http://www.ico.gov.uk/for\\_organisations/privacy\\_and\\_electronic\\_communications/the\\_guide.a\\_spx](http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide.a_spx)
3. ASA Code of Practice: <http://www.cap.org.uk/The-Codes/CAP-Code/CAP-Code-pdf-versions.aspx>
4. Readers might be interested in “Privacy and electronic communications – 2010” which shows the options that could protect privacy on the internet were ignored by the Government (e.g. consent requirements for behavioural marketing). Also “Reclaiming Privacy on the Internet – 2009” which describes how IP addresses and URLs can be transformed into personal data at any time by the user. Both documents are downloadable: from <http://www.amberhawk.com/policydoc.asp>

## ADVERT

### COURSES FOR PRIVACY PRACTITIONERS OR DATA PROTECTION OFFICERS

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection which can be held on-site. **We are the only course provider that delivers the data protection ISEB syllabus in public courses to ISEB's recommended length of time; all other provides reduce a 40 hour syllabus to 30 hours or less.**

With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, CCTV, human resources, data sharing, direct marketing) or targeted at specific staff members (e.g. managers) or on specialist aspects (e.g. social work functions, anti-fraud functions).

We have day long public courses in Data Protection Audit, Privacy Impact Assessments and RIPA as well as our popular, twice yearly, UPDATE session in London.

We will be soon delivering courses to ISEB's syllabus on Information Security Management (useful to those involved in implementing ISO27002 and HMG Security Framework)

If interested in any of the above please contact us at [info@amberhawk.com](mailto:info@amberhawk.com)

### COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification. **We are the only course provider that delivers the FOI ISEB syllabus in public courses to ISEB's recommended length of time; all other provides reduce a 40 hour syllabus to 30 hours or less.**

With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies.