Legal Update

Marketing by e-mail? A review of some important rules

Received (in revised form): 22nd September 2011

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 and other aspects information law.

ABSTRACT This article reviews the Information Commissioner's 'Guide to the Privacy and Electronic Communications Regulations' in the context of electronic marketing, especially marketing by e-mail. It also describes how these Regulations augment the marketing obligations under the Data Protection Act.

Journal of Database Marketing & Customer Strategy Management (2011) **18**, 322–325.

doi:10.1057/dbm.2011.31; published online 14 November 2011

Keywords: electronic marketing; PECR; e-mail marketing; soft opt-in; privacy; spam

The Information Commissioner has recently published a 'Guide to the Privacy and Electronic Communications Regulations' (the 'Guide')¹; this article reviews some of the content of this guidance in the context of e-mail 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.

PECR ADDS TO THE DATA PROTECTION ACT MARKETING OBLIGATIONS

Absent from the Guide is a reminder that an e-mail address is most likely to constitute

personal data as the data contains an identifiable name and the employer of a sender (for example, chris.pounder@amberhawk.com). Some e-mail addresses might be of a very confidential nature depending on the employer (for example, fred.bloggs@huntingdon_life_sciences.com) or if the individual has some kind of risk status (for example, e-mail addresses of individuals in witness protection).

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

- when e-mail addresses are collected and *before* they are collected, the identity of the organisation wanting to use the e-mail address and the marketing purpose must be identified to each individual who provides their e-mail address. Such information, or privacy notice, has to be prominent and clear in meaning (for example, not buried in the text of a web-form or couched in obscure language);

Correspondence:
Dr CNM Pounder
Amberhawk Training Ltd,
6/7 Feast Field, Horsforth,
Leeds, West Yorks LS18 4TJ
E-mail: chris.pounder@amberhawk.com

- any third-party marketing (for example, where an organisation lets other companies use its e-mail 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 (for example, click the send button). Doing nothing is not consent (for example, 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 (for example, marketing by e-mail) and either an 'opt-out' (for example, please tick the box if you don't want marketing) or 'opt-in' provided (for example, 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 (for example, towards 'opt-in');
- if an individual objects to the use of his e-mail address for a marketing purpose, then that objection prevails. There should be no more marketing e-mails 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 (for example, e-mail addresses should be kept up to date, secure and deleted when not needed).

In addition, the Advertising Standard 'UK Code of Non-broadcast Advertising, Sales Promotions and Direct Marketing' applies to the use of e-mails for a marketing purpose. Of particular relevance to most readers in the commercial sector will be Sections 8–10 (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 e-mail. '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, e-mail, 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 above).

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 e-mail addresses. Most likely, you would have distributed these e-mail 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

cannot 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 of the individual subscriber but users of a corporate subscription do not.

For instance, suppose the Bloggs Family have a subscription to 'btinternet.com'. The family's e-mail addresses are distributed to: a.bloggs@btinternet.com, b.bloggs@btinternet.com and c.bloggs@btinternet.com. If two of these individuals are users – can you identify the subscriber? Of course you cannot. So if a marketing person compiles a list of domestic e-mail addresses, and sends an unsolicited e-mail 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 (for example, chris.pounder@amberhawk.com, 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 e-mail is an e-mail that is not *solicited*. The Guide defines a *solicited* message is '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 e-mail.

But what happens if an individual subscriber does not tick an 'opt-out' box on a form (for example, if you do not want

to be contacted for a marketing purpose by e-mail, please tick the box). Does this mean any marketing e-mail is solicited or unsolicited? Well this depends on who is doing the e-mail marketing and the products being offered!

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 e-mails to an individual subscriber without an 'opt-in'.

These circumstances are:

- the organisation has obtained the e-mail 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 e-mail only relates to material that describes the organisation's similar products and services;
- each individual providing his e-mail address is given a simple means of refusing (free of charge except for the cost of transmission) the use of the e-mail address for marketing purposes; and
- when the e-mail address was initially collected the individual did not refuse the use of those details for a e-mail marketing purpose (see the data protection elements above if the e-mail 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 e-mails that promoted the products of another company in the same group, or if customers are asked to provide the e-mail addresses of their friends for a marketing list. Obviously, if the individual subscriber objects to the e-mail marketing, then any further marketing communication by e-mail will be *unsolicited*.

RULES THAT APPLY TO ALL MARKETING E-MAILS

There are two other rules associated with *any* e-mail marketing that are worth mentioning.

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

If e-mail 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, before 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. Therefore, 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 United Kingdom – they do not apply to spam e-mails, which are usually sent from abroad. However, having said that there is cause for limited optimism. First, 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 United Kingdom. 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 e-mails 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 do not sell those shares in spam filter software providers yet. However, if your organisation does e-mail marketing into Europe, or you are based in the United Kingdom, you **MUST** look at these rules or the national equivalent.

FURTHER READING

ASA Code of Practice: www.cap.org.uk/The-Codes/CAP-Code/CAP-Code-pdf-versions.aspx

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 (for example, 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 www.amberhawk.com/policydoc.asp

NOTE

- 1 Guide to the Privacy and Electronic Communications Regulations, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide.aspx.