Direct marketing – The new rules

Ruth Boardman, solicitor, Bird & Bird

The majority of this paper focuses on the provisions in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the “E-Privacy Regulations”) on the use of phone, fax, SMS and – especially – e-mail for direct marketing, and how these issues are addressed in the new Guidance on the E-Privacy Regulations issued by the Information Commissioner’s Office in November 2003 (the “Guidance”).

However, before looking in some detail at these provisions, the paper considers those sections in the general Data Protection Act 1998 that apply to direct marketing. The paper also provides an overview of the other provisions in the E-Privacy Regulations. These are as follows:

- Provisions specific to electronic communications service providers; and
- Provisions governing the use of cookies and similar technology.

Finally, it is very important that an organisation carrying out a direct marketing campaign by e-mail does not overlook other relevant legislation. Accordingly, the paper looks briefly at the most pertinent provisions in the general Data Protection Act 1998. It also highlights where there is a need for direct marketers to consider the Electronic Commerce (EC Directive) Regulations 2002, the Consumer Protection (Distance Selling) Regulations 2000 and the British Code of Advertising, Sales Promotion and Direct Marketing.

1. THE OLD LEGAL FRAMEWORK

The Data Protection Act 1998

1.1 An organisation will need to consider notification (i.e. registration), compliance with the data protection principles and individual’s rights. A comprehensive review of all of this is too extensive to be covered by this paper. I have considered the following provisions in some detail, as they are of particular relevance to direct marketing:

- fair obtaining;
- consent; and
- opt-outs.
Direct Marketing

1.2 Before looking at these provisions, though, it is useful to look at what the DPA, and the Information Commissioner, consider amounts to direct marketing.

1.3 Section 11 of the DPA defines direct marketing as:

“The communication (by whatever means) of any advertising marketing material which is directed to particular individuals”.

1.4 The Commissioner’s Guidance (p.3) considers that:

“The term “direct marketing” ... [covers] a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation’s aims and ideals. This would include a charity or a political party making an appeal for funds or support and, for example, an organisation whose campaign is designed to encourage individuals to write to their MP on a particular matter or to attend a public meeting or rally”.

Fair obtaining (DPA, Sch. 1, Part II, para 2)

1.5 The fair obtaining code is set out at Schedule 1, Part II, paragraph 2 – 3 of the DPA and provides as follows:

“2 (1) Subject to paragraph 3, for the purposes of the first principle [fair and lawful processing] personal data are not to be treated as processed fairly unless –

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph 3, and

(b) in any other case the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph 3.

2 (2) In sub-paragraph 1(b) “the relevant time” means –

(a) the time when the data controller first processes the data, or

(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged –

(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,

(ii) if within that period the data controller becomes, or ought to become aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or
(iii) in any other case, the end of that period

2 (3) The information referred to in sub-paragraph 1 is as follows, namely

(a) the identity of the data controller,

(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,

(c) the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.”

1.6 To summarise, each data subject must be provided with the following information:

- the data controller’s identity;

- details of any UK representative (this is only likely to be applicable to data controllers established outside the EEA);

- the purposes for which the data are to be processed – i.e. for direct marketing; and

- any other information which, in the specific circumstances is necessary for the processing to be fair.

1.7 It is not necessary to include information that is already known to the individual. So, for example, if an individual has supplied a name and address in order to receive a catalogue that they themselves have requested, it is not necessary to explain that the information will be used to issue the catalogue. It is only additional, non-obvious, uses that must be explained. This provision is not set out clearly in the DPA itself. It is, however, clear in the Data Protection Directive. Article 10 of this states that the obligation to provide information to a data subject does not apply where the data subject already has that information.

1.8 The final element of the fair processing code obliges data controllers to provide any other information which, in the circumstances, is necessary. Again, the Directive gives some guidance as to the types of information that may be required here. Article 10 suggests that this may include information as to:

- the recipients, or categories of recipients, of the data;

- whether replies to the questions are obligatory or voluntary and the consequences of failing to provide requested information; and

- the existence of a right of access to and the right to rectify the data concerning the data subject.
1.9 These items are not mandated. However, the Directive specifically notes that they may be necessary in particular circumstances.

**Timing of the Notice**

1.10 The fair processing code specifically considers the time at which the fair processing notice must be given. The Code contains quite complicated provisions as to when a fair processing statement must be given where information has not been obtained directly from the relevant data subject. In essence, in this situation, the data controller should provide the notice when they first process or disclose the data. There is an exemption from the fair processing code for this type of information where provision of the fair processing statement would involve a disproportionate effort or where the data controller is obliged to process the information in order to comply with any non-contractual legal obligation. This exemption has been modified by the Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000\(^3\). This provides that the exemption does not apply if a data controller has received notice from an individual asking for the fair processing information. Furthermore, where the data controller is relying on the disproportionate effort exemption then the data controller must record the reasons why they believe the exemption will apply.

1.11 The DPA does not set out when the fair processing information must be provided where data are obtained directly from a data subject. However, the Commissioner’s guidance on this point follows the principles set out in the *Innovations* case (see below) – namely that the information must be provided before or at the time that the customer provides the information. Anyone conducting a telemarketing campaign to consumers which could lead to contracts being concluded at a distance should also note Reg 7 (4) of the Consumer Protection (Distance Selling) Regulations 2000 (SI2000 No 2334) which requires the identity of the caller and the commercial purpose of the call to be made clear at the beginning of the call.

1.12 The Commissioner issued guidance on what information should be provided in a fair processing statement in a number of different papers. (For example, there is guidance on privacy statements to be used on the Internet in the *Commissioner’s Website FAQs*). Organisations preparing fair obtaining statements would, therefore, be well-advised to check the Commissioner’s website for guidance relevant to them.

1.13 In addition to specific guidance on the DPA, the Commissioner also issued guidance on direct marketing under the Data Protection Act 1984. This guidance headed *Data Protection Guidance for Direct Marketers*, is still largely relevant today and is the most comprehensive statement from the Commissioner’s Office as to the impact of data protection on this industry.\(^4\) The following provisions in this guidance are of particular note:

- The Commissioner will have regard to the location and prominence of any fair obtaining notice. He will consider where it is placed, the font size of the

---

\(^3\) SI2000 Number 185.

\(^4\) Not all of the guidance is applicable. In particular, the old guidance states that data controllers can usually assume that individuals would expect to receive marketing information from companies with whom they trade and that there is no need to state this. This is no longer a correct statement of the law. The guidance also discusses business-to-business marketing exemptions – that no longer apply under the DPA.
statement and whether it is suitable for the particular group that is likely to read it. For example, far greater clarity will be required if information is to be collected from children.

- The notice must state if information will be disclosed to third parties (i.e. list rental).

- A statement if more than merely name and address information will be provided to third parties. (Merely telling individuals that details will be disclosed to third parties may not sufficiently alert them to the fact that, for example, account information or trading information may be disclosed to third parties).

- This statement should make clear if the data controller will use the information itself to market unconnected products and services.

- The statement should state if information will be disclosed to group companies. Furthermore, where the group does not have a strong public identity then it will be necessary to explain which companies are comprised in the group. In other words, a statement that “We may share data within our group” is often not sufficiently clear.

- If host mailings will be carried out on a selective basis then this should be made clear. This would apply if the data controller intends to include inserts in material on a selective basis on behalf of third parties. For example, a bank may agree to carry out a host mailing on behalf of a luxury goods retailer to high net worth individuals. The Commissioner is particularly keen that data controllers should draw attention to this practice. This is because individuals who respond to targeted host mailing of this kind will often inadvertently be disclosing information to the person to whom they respond. For example, if an individual respond to a leaflet that has been sent on a selective basis to individuals whose current account regularly contains in excess of £5,000 then, by responding to the leaflet, they will be inadvertently disclosing to the leafletter that they fall into this category (as the leafletter will know that the leaflet was only sent to individuals who satisfy this criteria).

- If the information is going to be used for direct marketing by intrusive means – such as telephone or personal visits – then this should be made clear.

- Do not mislead individuals into providing marketing information by giving the impression that they are taking part in an anonymous market research survey.

- Where a “refer a friend” scheme is used, then the Commissioner would consider whether the scheme is fair both to the individual providing the information and to the friend referred. The Commissioner concludes that such schemes are acceptable where the source may reasonably be expected to be aware of and to respect the wishes of the friend they are referring. If, however, the person referring the friend is unlikely to be aware of the data subject’s wishes then the scheme is unlikely to be acceptable. The Commissioner was also sceptical about schemes where an individual is offered an inducement (such as a money off voucher) to refer a friend.
List Rental

1.14 Where an organisation buys in marketing lists from a third party, then it must rely on the third party having given appropriate notice to the individuals whose details are contained in the list. If the list broker obtained the information without doing this then the information will not have been obtained fairly.

1.15 Again, this is covered in the guidance given by the Commissioner under the 1984 Act. The Commissioner suggested that organisations buying marketing lists should make sure that their contracts require the list brokers to provide fair processing information to individuals – and that a “fair obtaining warranty” is included in the contract to this effect. The Commissioner also expected that data controllers would take steps to monitor a list broker’s compliance with this obligation. If an organisation disregards evidence that a list broker has obtained information without providing the necessary fair processing statements or fails to obtain a fair obtaining warranty then the Commissioner may well conclude that unfair processing is taking place. Processing will also be unfair if a data controller removes any “do not mail” or “do not rent” suppression markers from the list broker’s database.

1.16 There is also case law under the 1984 Act on data protection and direct marketing – especially the British Gas and Innovations cases. These cases are considered briefly below.

1.17 The British Gas case related to the appeal by British Gas Trading Limited (“BGTL”) against an enforcement notice issued by the Commissioner.

1.18 In 1997 BGTL issued a leaflet to all its gas customers with their quarterly gas bill. The leaflet said that BGTL would like to write to its customers about its present range of products and services and any future ones, and to pass customer details to companies within its group. It suggested that customers should complete and return a coupon if they did not wish to receive this information. In order to send out these leaflets BGTL processed customers’ personal data. This personal data had been collected from the gas bill database.

1.19 The Tribunal decision considered the following points:

- There is a significant distinction between utilities and other general commercial organisations, since customers have no choice but to provide their personal details to receive a utility service. Processing for gas related marketing purposes would be fair. Processing for purposes wider than those which would have been obvious to the customer at the time of supply of his information without his consent would not be fair. Expectations as to the scope of goods and services to be marketed by a particular supplier would change over time and this should be taken into account when examining fairness.

- It would be fair for BGTL to process customer data obtained as a result of supplying gas for:

---

5 British Gas Trading Limited v the Data Protection Commissioner March 25th 1998
6 Innovations (Mail Order) Limited v Data Protection Registrar Case DA/9231/49/1
@ Ruth Boardman 2004
The moral rights of the author have been asserted
Database right The Centre for International Law (maker)
• continuing its supply of gas;
• marketing and host mailing information on gas related matters; and
• marketing and joint promotion with third parties of electricity related products where these are associated with the marketing or promotion of gas where the processing would not lead to any disclosure of personal data by BGTL to a third party.

The point was made that BGTL would be able to inform new customers of the type of marketing intended and provide them an opportunity to object either orally, or in an electronic or other communication to be returned. Specific reference was made to an opt-in box ticked or an opt-out box left blank.

With existing customers, where the relationship began in monopoly conditions, the Tribunal did not consider it sufficient to merely send the customer a leaflet providing them with an opportunity to object to data being processed for purposes beyond gas related purposes. The Tribunal considered it would be sufficient for customers to be informed of the type of marketing or promotions which would be carried out, given an opportunity to consent then and there. Alternatively, the Tribunal considered that where a document had to be returned to BGTL in any event, then an opt out box could be used.

The Innovations case considered the timing of the fair obtaining notice.

In the Innovations case, the Data Protection Tribunal scrutinised Innovations’ practice of only informing customers of the fact that their personal details would be used for list rental purposes at the point at which they received an acknowledgement of receipt of the order. Although individuals could object to the list rental by writing to Innovations, the Tribunal took the view that it was not fair to explain this to individuals at such a late stage. Notification had to be given to the data subject before he or she supplied the data controller with the personal data for that purpose. The Tribunal considered that it would be possible to do this by including a statement in advertisements, or by limiting its list to customers placing orders subsequent to receipt of the acknowledgement.

The Tribunal also made clear that when considering what would be fair to the data subject, the data controller must consider for how long the individual would recall that their information had been passed to the data controller and that, therefore, his personal data would be traded. It was concluded that this was unlikely to extend beyond six months.

Consent (DPA, Schs 2 & 3)

An organisation may have to obtain consent (i.e. an opt-in) to carry out certain forms of direct marketing. Consent may be required as a result of the first data protection principle (fair and lawful processing).

The first data protection principle states that data controllers may not process any personal data unless they can satisfy one of the conditions set out in Schedule 2 to the DPA and, where sensitive data are concerned (e.g. health data), one of the additional conditions in Schedule 3 to the DPA. The obligations to process personal data lawfully
also brings in compliance with the law of confidence; this may also result in a need to obtain consent.

**Schedule 2 and 3 conditions**

**Schedule 2 conditions**

1.26 The Schedule 2 conditions apply to all personal data used for direct marketing. The conditions are broad and organisations conducting direct marketing should have no difficulty in satisfying a Schedule 2 condition. The condition which the Direct Marketing Association thinks is most applicable is Schedule 2 paragraph 6:

> "The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data was disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject".

Provided that a data controller has given opt-out information (as to which see below) then this condition will probably be easy to satisfy.

**Schedule 3 conditions**

1.27 Where a data controller wishes to process sensitive personal data for direct marketing, then it must also satisfy one of the conditions in Schedule 3. Sensitive personal data relate to an individual's health, religious or similar belief, the commission of criminal offences and related proceedings, racial or ethnic origin, sexual life, and trade union membership. This list is exhaustive. Accordingly, information that one may colloquially talk about as being sensitive (primarily financial information) does not count as sensitive data for the purposes of the DPA. (There may, however, be other legal restraints on the use of such information – as to which see below). A data controller will have far more difficulty in satisfying one of the Schedule 3 conditions. Although there are a number of Schedule 3 conditions, in practice, the only one on which data controllers are likely to be able to rely for direct marketing purposes is explicit consent. The Data Protection Directive, which the DPA implements, states that consent means “any freely given specific and informed indication of his wishes by which a data subject signifies his agreement to personal data relating to him being processed”. Based on this provision, the Information Commissioner’s advice is that:

- sufficient information must have been given for the consent to be meaningful; and

- that one cannot infer consent from a failure to object. In other words, if an organisation wishes to use sensitive personal data for direct marketing then it must obtain the active consent of the individual concerned. It cannot notify the individual that it will use the information for this purpose unless they object. In practice, this means that a tick box opt-in approach will be necessary where, for example, an organisation wishes to conduct direct marketing campaigns to individuals who are known to suffer from a particular condition.
Lawful processing - confidentiality

1.28 In addition to complying with the Schedule 2, and where applicable Schedule 3 conditions, a data controller must also process personal data in accordance with any other relevant legal considerations. This is likely to be of particular relevance where confidential information is concerned. There is no fixed definition of what constitutes confidential information – as it is decided on a case-by-case basis. The information must, however:

- not be of a merely trivial nature; and
- have been imparted in circumstances of confidentiality.

Certain classes of information have been widely recognised by the law as being confidential – this would include information given to a health professional and financial information held by a bank, building society or other financial services provider. Where information is confidential then it may not be disclosed outside the organisation and may not be used for a purpose other than the purpose for which it was obtained. It is this latter restriction which is particularly important to organisations carrying out direct marketing in the financial services sector. Organisations will only be able to use financial data for direct marketing if this is in accordance with the purpose for which the data were provided or if they have obtained the individual’s consent.

1.29 The Information Commissioner gave guidance on this area under the Data Protection Act 1984. Again, much of this guidance will still be of relevance today. The Commissioner’s guidance was that individuals would probably only expect financial services providers to use information to market products or services that are directly related to those that the customer has asked to receive.

1.30 The Commissioner gave two examples that explain how he will apply this approach.

- In the first example, a bank is aware that a customer has a regular surplus in their current account of £1,000. The bank is also aware from its Visa card holder records that the customer settles their account promptly at the end of every month. The bank uses this information to offer the customer the opportunity to open a deposit account and to upgrade their ordinary Visa card to a “gold card”. The Commissioner considers this to be unobjectionable – even though the information is confidential. This is on the basis that the information is only used to make an offer that is consistent with the level of service a customer might reasonably expect from their bank and with the bank’s responsibility to provide proper financial information and advice.

- By contrast, if a bank analyses the types of transactions which customers have made by categorising types of purchase made by Visa card and then enters into joint marketing arrangements with a number of third parties to market related products (for example by offering membership of a wine club to cardholders who regularly buy wine) then, in the Commissioner’s view, this is likely to amount to a breach of confidentiality. This is on the basis that customers would probably not have expected transaction information to be analysed in this way. This offer is not part of the service that the customer would expect to have received from
the card issuer. Further, the Commissioner thinks it is objectionable that the financial benefits of the exercise accrue primarily to the card issuer rather than the customer.

1.31 For this reason, where organisations wish to use financial data for direct marketing then it would be advisable to obtain the individual’s consent to this at the outset of the relationship. As the relevant legal consideration here is the common law of confidentiality, rather than the DPA, an organisation could rely on implied consent – in other words it would not need to obtain the explicit or opt-in consent method mandated for sensitive personal data by the DPA. An organisation must, however, tell individuals in advance that it intends to use data for this purpose even to rely on implied consent; unless an individual has been told how data will be used they cannot possibly be said to have given any form of consent.

Opt-outs (DPA, S 11)

Section 11 of the Act: the right to object to direct marketing

1.32 The Act grants individuals the right specifically to prevent direct marketing in section 11. Further, individuals can require an organisation not even to start conducting direct marketing to them. An individual must exercise this right by giving notice in writing (which could be given by e-mail). The data controller is then allowed a reasonable period of time to comply with the request. If the data controller refuses to comply with the request then the individual could, ultimately, enforce his or her right through the court. Alternatively, they may request the Information Commissioner to “conduct an assessment”.

1.33 Individuals sometimes think that the DPA grants them a right to require an organisation to delete all data held about them – in other words to stop processing all information about them. This is not correct. Although the DPA does grant rights to prevent certain types of processing (where this would cause substantial damage or distress and would be unwarranted) there is no general right to require data to be deleted. In fact, it would be counter-productive to delete all data relating to an individual who did not wish to receive direct marketing information, as there would then be no way of ensuring that the individual was not subsequently added to a direct marketing list. The Information Commissioner’s Office gave advice on this under the Data Protection Act 1984, which is still relevant. This said that organisations would be best advised to comply with this right by using suppression/de-duplication software. Data controllers will therefore need to record any objections sent to them and de-duplicate marketing databases before conducting any direct marketing exercises.

Electronic Commerce Regulations

1.34 Certain organisations will also have to have regard to the provisions of the Electronic Commerce (EC Directive) Regulations 2002 (SI2002 No 213). The Regulations apply to organisations providing information society services, which are defined at Reg 2 (1) as:

“any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service”.

@ Ruth Boardman 2004
The moral rights of the author have been asserted
Database right The Centre for International Law (maker)
1.35 The Electronic Commerce (EC Directive) Regulations apply to persons providing services that are normally provided for remuneration, whereas the E-Privacy Regulations apply to anyone who makes use of these particular media in order to promote themselves.

1.36 The Electronic Commerce (EC Directive) Regulations also only apply to “commercial communications”. These are defined as:

“a communication, in any form, designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial or craft activity or exercising a regulated profession … [subject to exceptions].”

1.37 For an organisation engaged in business activities, it would find that most of its promotional activities would fall within this definition. However, charities and political parties in particular would not be caught by this (unless they engage in trading activities).

1.38 Organisations that provide financial services that are subject to regulation by the Financial Services Authority under the Financial Services and Markets Act 2000 would need to have regard to specific regulations that apply to them in place of the Electronic Commerce (EC Directive) Regulations.

1.39 Organisations to whom the Regulations apply would need to comply with Reg 8 when sending promotional e-mails. This regulation provides that any unsolicited commercial communications sent by e-mail are “clearly and unambiguously identifiable as such as soon as … received”. The Electronic Commerce Directive which the Regulations implement suggests that this may mean marking the “envelope” of the e-mail. The aim of the Regulations is to ensure that persons receiving promotional e-mails are aware that this is what they are before they open the e-mail – as the act of opening the e-mail obliges the recipient to incur the additional costs of collection time. The net effect of this provision is that organisations sending promotional e-mails have to make sure that the subject line of the e-mail alerts the recipient to the fact that it is promotional. This is not as onerous as it first sounds. There is an equivalent obligation under the British Code of Advertising Standards and Promotion (as to which see post). In a ruling relating to the Training Guild, the Advertising Standards Authority considered that an e-mail headed “Business Seminars – Telesales & Selling Skills Made Easy” complied with this requirement. In other words, it is not necessary to include the words “advert”, or equivalent, in the subject heading.

1.40 Reg 8 is supplemented by Reg 7 which applies to all commercial communications which form part of an information society service whether or not they are sent by e-mail. Again, it requires that all commercial communications are clearly identifiable as such. Furthermore, they must clearly identify the person on whose behalf the communication is sent and must clearly identify as such promotional offers, competitions and games and must ensure that the conditions relating to such promotions are easily accessible and presented clearly and unambiguously.

1.41 Organisations providing information society services should, of course, also be aware of the provisions in the Electronic Commerce (EC Directive) Regulations that set out information that must be made available about the service provider (Reg 6), about the way in which the contract may be concluded (Reg 9) and about the acknowledgment of orders and the correction of errors (Reg 11). In most cases, information society service
providers would address the requirements of these Regulations via information on their website, through which any e-commerce transactions would be concluded.

**Consumer Protection (Distance Selling) Regulations 2000**

1.42 Organisations carrying out direct marketing to consumers must also be aware of the Consumer Protection (Distance Selling) Regulations 2000. There are parallel regulations that apply to organisations providing regulated financial services. These Regulations apply where an organisation will conclude a contract with a consumer at a distance. Again the Regulations impose information obligations on service providers (Reg 7) which requires information to be provided about a supplier, the goods or services, pricing information, cancellation rights, validity periods for any offers, length of contract, and substitution arrangements.

1.43 Much of this information must be provided in writing or in another durable medium which is available and accessible to the consumer in order to comply with Reg 8. Reg 8 also obliges the service provider to give information about cancellation arrangements, a point of contact for complaints and information about after sales service and guarantees.

**British Code of Advertising, Sales Promotion and Direct Marketing**

1.44 In addition to complying with the legislation mentioned earlier, direct marketers must also comply with the British Code of Advertising, Sales Promotion and Direct Marketing. The 11th edition of this came into force on 4 March 2003. Although the bulk of the Code is concerned with the content of advertisements (for example ensuring that marketing is legal, decent, honest and truthful) there are also specific rules on the way in which communications must be sent, on the information that must be provided and when consent is necessary to carry out marketing and so forth. In effect, the Code acts as a summary of all the legislation discussed elsewhere in this paper. The Code is enforced by the Advertising Standards Authority. Breach of the Code is likely to lead to substantial adverse publicity and may lead to the loss of publishing space, to the loss of trading discounts or to the requirement for marketing communications to be pre-vetted by the CAP copy advice team.

2. **BACKGROUND TO THE E-PRIVACY REGULATIONS**

2.1 On 15 December 1997 Directive 97/66/EC was adopted (the “Telecoms Data Protection Directive”). This concerned the processing of personal data and the protection of privacy in the telecommunications sector. In the UK, the Telecoms Data Protection Directive was implemented by the Telecommunications (Data Protection and Privacy) Regulations (the “Telecoms Privacy Regulations”), most of which came into force on 1 March 2000. The Telecoms Data Protection Directive and the Telecoms Privacy Regulations particularised the provisions of the general Data Protection Directive and the Data Protection Act 1998 for the telecommunications sector. While most of the provisions related specifically to telecom service providers (for example provisions relating to itemised billing and directories), some of the provisions applied to anyone who used telecommunications services for direct marketing.

2.2 It rapidly became apparent that the Telecoms Data Protection Directive was out of date. In particular, there was significant uncertainty as to whether the Telecoms Data
Protection Directive only applied to voice telephony or whether its provisions would also extend to e-mail and the Internet. This confusion arose because the Telecoms Data Protection Directive used the term “call” and a number of member states (including the UK) interpreted this as only referring to traditional circuit-switched connections and not to packet-switched transmissions (i.e. as only applying to traditional voice telephony and not to data transmission or use of the Internet). In the UK, there were some disagreements between the Information Commissioner’s Office who wished to adopt a broad interpretation of the Telecoms Data Protection Directive and the Department of Trade and Industry (who adopted a restricted view).

2.3 Accordingly, on 25 June 2002, the Council of the European Union formally adopted the Electronic Communications Privacy Directive 2002/58/EC (the “E-Privacy Directive”). The E-Privacy Directive updates and extends the scope of the Telecommunications Privacy Directive so as to make clear that it does indeed include e-mail and SMS. In addition, it introduces new restrictions on the use of cookies and similar technology and extends obligations on communications service providers.

2.4 The UK has implemented the E-Privacy Directive through the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (the “E-Privacy Regulations”). The E-Privacy Regulations came into force on 11 December 2003. Save in relation to certain limited provisions relating to printed directories, there are no transitional provisions in the E-Privacy Regulations. Accordingly, as from 11 December, they apply both to direct marketing carried out in relation to new prospects whose details have been obtained after that date and to direct marketing carried out via an electronic communications network to existing prospects whose details were obtained before that date.

3. NEW DIRECT MARKETING RULES

3.1 Regulations 19 to 26 of the E-Privacy Regulations relate to direct marketing. The DTI had the opportunity, with the implementation of the E-Privacy Directive, to simplify previous rules relating to direct marketing by means of telecommunications services. However, perhaps regrettably, the DTI has not taken advantage of this opportunity. The E-Privacy Regulations, like the earlier Telecoms Privacy regulations, set out a relatively complex framework, which grants people different rights depending on whether they are individual subscribers or corporate subscribers and depending on the medium used for the direct marketing.

Solicited v Unsolicited

3.2 The restrictions on the use of fax machines, e-mail and public electronic communications services for direct marketing at Regulations 20-22 of the E-Privacy Regulations apply to “unsolicited” communications and calls.

3.3 The Guidance considers what is meant by an unsolicited communication or call. The Guidance poses the following question:

“What is the difference between a “solicited marketing message” and “unsolicited marketing message that you consent to receiving”?”
3.4 The Guidance answers as follows:

“Put simply, a “solicited message” is one that you have actively invited. An “unsolicited marketing message that you consent to receiving” is one that you have not specifically invited but you have positively indicated that you do not mind receiving it. This is not the same as failing to object to receiving a message when you are given the opportunity to object”.

3.5 This explanation confuses rather than clarifies. However, the Guidance goes on to give the following helpful explanation:

“By analogy, it is the difference between asking someone to buy you a drink and that person asking you if they may buy you a drink to which you answer “Yes”. The outcome may be the same in both scenarios – you receive a drink. However, in the first scenario you have invited the drink whereas, in the second scenario, you haven’t objected to someone buying you a drink but you didn’t invite them to make the offer. To extend the analogy, when a person does not say no a drink that is offered, it is not the same as saying yes. They may simply be ignoring the offer which they are entitled to do if it doesn’t interest them”.

Individual Subscribers

3.6 Most protection is given to individual subscribers, who unlike corporate subscribers, have an enforceable right to opt-out under the Regulations. However, this does not mean that the focus of the Regulations is on direct marketing to consumers. The E-Privacy Regulations define “individual” as follows:

““individual” means a living individual and includes an unincorporated body of such individuals”.

Accordingly, individual subscribers will include private individuals – but will also include sole traders (living individuals) and partnerships (which are, in England and Wales, unincorporated bodies of individuals). The provisions in the E-Privacy Regulations relating to corporate subscribers only apply to subscribers who are:

“a. a company within the meaning of Section 735 (1) of the Companies Act 1985;
b. a company incorporated in pursuance of a royal charter or letters patent;
c. a partnership in Scotland;
d. a corporation sole; or
e. any other body corporate or entity which has a legal person distinct from its members”.

The effect of this is that organisations that solely carry out B2B marketing will still have to consider the impact of the Regulations if their marketing databases contain prospects who are sole traders or partnerships. As there are quite substantial organisations that trade through partnerships (e.g. professional services firms) it is likely that the E-Privacy Regulations will apply to many organisations that only conduct B2B marketing.
Furthermore, the Regulations do provide that e-mail marketing to corporate subscribers must still identify the sender and provide contact details, and marketing to corporate subscribers which involves the processing of personal information (i.e. when it is sent to a named person) that individual will have an enforceable right under the DPA to have the marketer cease sending them marketing material.

**Consent**

3.7 In a number of places, the E-Privacy Regulations require consent to be obtained, before (e.g. e-mail marketing to individual subscribers) may be carried out. The general Data Protection Directive, which the E-Privacy Directive particularises, defines consent at Article 2 (h), as

“any freely given specific and informed indication of his wishes by which a data subject signifies his agreement to personal data relating to him being processed”.

3.8 The Commissioner’s Guidance, following on from the requirement in the Directive that consent must be “signified” explains that consent

“... is where you actively sign up for something and where you know what you are signing up to. There may be a number of ways to indicate consent. For example, where you tick a box as a positive indication that you agree to receiving marketing ...” (p.2).

**Opt-in**

3.9 The example given in the Guidance is commonly referred to an “opt-in”. This paper (and the direct marketing industry) often talk about “opt-in consent”. The E-Privacy Regulations do not, however, insist that consent is obtained via an opt-in. As the Guidance makes clear, consent may also

“involve clicking an icon, sending an e-mail or subscribing to a service”.

**Opt-out**

3.10 By contrast, an opt-out requires an individual to tick a box to register their objection to receiving direct marketing. This does not satisfy a requirement for consent. It is, though, sufficient to comply with certain provisions in the Regulations that grant a right to object.

**Direct Marketing by Telephone (Regulation 21)**

3.11 Regulation 21 (1) grants all subscribers – individuals and corporates – rights to object to unsolicited calls for direct marketing purposes.

**Fax Marketing (Regulation 20)**

3.12 Regulation 20 (1) (a) prohibits organisations from sending direct marketing faxes to individual subscribers unless the individual subscriber has notified the direct marketer that he/she consents to receiving such communications. The Regulations provide that the subscriber must have notified the direct marketer – that is that the subscriber must have taken active steps to give consent. This imposes an opt-in consent requirement for direct marketing to individuals by fax. (In other words, this means that the individual must tick
a box to signify their agreement to receiving direct marketing by fax, as opposed to ticking a box to show that they object to receiving such material).

3.13 Corporate subscribers are given a right to object to receiving direct marketing faxes (Regulation 21(b)) but their prior consent is not required. These provisions replicate those in the earlier Regulations.

*Automated Calling Systems (Regulation 19)*

3.14 Regulation 19 replicates provisions in the earlier Regulations which require organisations to obtain consent (i.e. an opt-in approach) if they wish to use automated calling systems. This opt-in approach applies both to individuals and to corporates.

3.15 Under the previous Regulations there was some uncertainty as to what was meant by an automated calling system. The Information Commissioner’s Office had issued guidance (in the context of promotional campaigns by political parties) suggesting that fax marketing and SMS marketing would fall within these provisions. This will not be the case under the E-Privacy Regulations, due to the new, helpful, definition of an automated calling system as set out in Regulation 19 (4). This provides that:

"... an automated calling system is a system which is capable of –

a. automatically initiating a sequence of calls to more than one destination in accordance with instructions stored in that system; and

b. transmitting sounds which are not live speech for reception by persons at some or all of the destinations so-called."

3.16 The Regulations would, therefore, continue to catch forms of technology which, so far, have been more prevalent in the US whereby entirely pre-recorded direct marketing calls are made by telephone. These calls have caused a particular problem in the US as the person receiving the call is unable to hang up until the recorded message has ended (as the person called cannot hang up while the caller remains on that line). This has led to some difficulties in the US when individuals have been unable to make calls to emergency services.

*Use of e-mail for direct marketing purposes (Regulation 22)*

3.17 The biggest change to direct marketing practices introduced by the E-Privacy Regulations is the restriction on e-mail marketing set out at Regulation 22. The regulation also applies to direct marketing communications sent by SMS, as e-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”.

3.18 The regulation only applies to communications sent to individual subscribers. However, as explained earlier, as this will protect subscribers who are sole traders or partnerships, the regulation will affect many organisations who only conduct B2B marketing. It is also worth noting that the DTI, in its consultation exercise that preceded the introduction of
the Regulations, specifically invited comments as to whether the Regulations should apply to corporates. The DTI’s published response to the consultation concluded that, on balance, it did not think it necessary to do this. However, the consultation paper specifically noted that the government would be prepared to review this decision in the light of working experience of the new rules. This is, therefore, an area that may be subject to change.

3.19 Regulation 22 (2) provides that direct marketing material may not be sent by e-mail unless the recipient has previously notified their consent (the “prior consent” rule). In other words, the Regulation introduces an opt-in regime.

The Soft Opt-In (Regulation 22(3))

3.20 There is a limited exception to the prior consent rule. It is set out at Regulation 22 (3) and provides that:

“A person may send or instigate the sending of electronic mail for the purposes of direct marketing where –

a. that person 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;

b. the direct marketing is in respect of that person’s similar products and services only; and

c. the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and where he did not initially refuse the use of the details, at the time of each subsequent communication”.

3.21 Somewhat confusingly, this opt-out regime is now almost universally referred to as the “soft opt-in”.

3.22 The exception is useful as it allows for the continued use of an opt-out in limited circumstances. However, there are a number of restrictions to the soft opt-in:

- It only applies to marketing prospects to whom there has been a sale or negotiation for a sale. It would not, therefore, cover pure contacts;
- The direct marketing must be carried out by the same person (i.e. legal entity) who obtained the original details;
- The direct marketing is limited to similar products and services; and
- The individual must have an offer to opt-out when their details were first obtained.

3.23 The Commissioner’s Guidance has been particularly on what constitutes “similar products and services”. The Guidance states on page 22 that:
“In our view, the intention of this section is to ensure that an individual does not receive promotional material about products and services that they would not reasonably expect to receive. For example, someone who has shopped online at a supermarket’s website (and has not objected to receiving further e-mail marketing from that supermarket), would expect at some point in the future to receive further e-mails promoting the diverse range of goods available at that supermarket”.

3.24 In other words, the ICO is taking a “purposive approach” to the phrase and applying its general approach to fairness.

3.25 The precise wording of the soft opt-in means that it cannot be used by organisations who wish to carry out marketing on behalf of third parties by e-mail. This is because the soft opt-in only applies where the direct marketing is in respect of direct marketers’ own products and services. It follows from this that the soft opt-in cannot usually be used by group companies or partnership loyalty schemes. Both of these issues are considered by the ICO (page 27 for group companies and page 28 for partnership loyalty schemes). The ICO’s conclusions here are not particularly surprising.

3.26 The ICO’s comments on the use of bought-in mailing lists are more interesting. The Guidance here is at pages 24 – 25. It is clear from the E-Privacy Regulations that the soft opt-in cannot be used by organisations using bought-in marketing lists. This is because the direct marketer must himself have obtained the recipient’s contact details in the course of sale or negotiations with that person.

3.27 Organisations wishing to use bought-in e-mail mailing lists would need to rely on the recipients having given consent to receiving e-mail marketing. Regulation 22 (2) permits e-mail marketing where “the recipient of the e-mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender”. The ICO focuses on the fact that permission must have been notified to the sender in relation to communications being sent by or at the instigation of the sender. If a third party has compiled a mailing list – even of individuals who have opted-in to receiving e-mail marketing from third parties – then the ICO takes the view that these requirements are not met. This is on the basis that the marketing prospect has not notified the sender of his consent. In the ICO’s view, therefore, third party mailing lists can only be used in relation to solicited marketing. This would mean that precise details of the third parties would have to be included, so that the prospects could be said to have solicited information from those third parties. The Guidance states as follows:

“… it is difficult to see how third party lists can be compiled and used legitimately after 11 December 2003 on any other basis than one where the individual subscriber expressly invites, i.e. solicits marketing by electronic mail”

3.28 It is an area where the E-Privacy Regulations and the ICO’s Guidance are more stringent than required by the Directive. Article 13 (1) of the Directive permits use of electronic mail for direct marketing “in respect of subscribers who have given their prior consent”. Likewise, Recital 40 merely talks about “prior explicit consent of the recipient”; there is no requirement that the consent is given direct to the sender of the marketing.

3.29 Organisations should have been offering opt-outs for many years in any event in order to comply with the provisions of the Data Protection Act 1998 and, before that Act, the Data
Protection Act 1984. It is, therefore, perhaps the other restrictions that may prove more limiting. Marketing departments will, understandably, wish to create value from their marketing lists by cross-marketing broader ranges of products and services, by marketing group company services and perhaps by host marketing third party products and services. None of these activities will be permitted on the basis of the soft opt-in. If this kind of marketing activity is of substantial significance to an organisation, then it may be forced into the hard opt-in approach, notwithstanding the exception

**Legacy Data**

3.30 The E-Privacy Regulations will, as of 11 December 2003, apply equally to new data collected after that date and to e-mail contact data collected before that date. Where organisations collect new data, they are able to construct data collection procedures in such a way as to obtain opt-in consent if this is necessary. Where organisations have existing databases then they may only continue to use those data for e-mail marketing if they can fall within the provisions of the soft opt-in. As has been seen above, the soft opt-in would not cover many typical forms of e-mail marketing carried out by organisations – such as marketing carried out by group companies or marketing to pure contacts, where there has been no previous sale or negotiations relating to a sale. If organisations cannot rely on the soft opt-in then they would need to re-approach marketing prospects to obtain opt-in consent. It seems probable that many people would not respond to a request for opt-in consent, although those same people may also not actively object to receiving e-mail marketing.

3.31 The Commissioner’s Guidance (see page 24) is helpful here. It takes the view that provided legacy data were obtained in accordance with privacy legislation enforced before 11 December 2003 and have been used recently, that they can continue to be used on an opt-out basis. Organisations would, however, have to comply with the other elements of the soft opt-in by including an unsubscribe option with every e-mail.

3.32 The ICO’s approach is helpful. It is, however, not consistent with the Advertising Standards Authority’s code of practice which does not have any leniency towards legacy data. We understand, informally, that the ASA is likely to revise its code in the light of the Guidance.

**Corporate Subscribers**

3.33 The general right, under the Act to object to direct marketing must not be overlooked when organisations review their direct marketing strategies for compliance with the E-Privacy Regulations. A person who does not have rights to object to receiving direct marketing under the E-Privacy Regulations will, of course, still retain their rights under the Act. An example is helpful to show how this works. An organisation may wish to send direct marketing material to Mr Smith who is the Chief Finance Officer for A Large Corporate PLC. The marketing material is to be sent by e-mail. The E-Privacy Regulations do not prevent the sending of marketing material to the target – as it is A Large Corporate PLC which has an account with an internet service provider. As A Large Corporate PLC is a corporate subscriber the opt-in requirements applicable to e-mail marketing under the E-Privacy Regulations are not relevant. However, Mr Smith retains his general rights to object to direct marketing under the Act. Accordingly, he
will be entitled to contact direct marketers who send material to him and insist that they cease doing this.

Preference Services

3.34 Regulations 25 and 26 continue the existence of the Telephone and Fax Preference Services. These allow subscribers who object to receiving direct marketing to register. Subsequent transmission of direct marketing material to these people is then a breach of the Regulations.

3.35 Whilst both individuals and corporates can register with the Fax Preference Service, the Telephone Preference Service is currently only available to individual subscribers (Regulation 26). However, this is an area that will change. The DTI has publicly committed to amending this so as to extend opt-out rights to corporates. However, before it does this it needs to re-negotiate the contract with the TPS. This is anticipated to take place in April 2004.

3.36 As with the earlier Regulations, registration with the TPS or FPS does not immediately ban direct marketing to that person. Instead, organisations have a 28 day grace period, during which it is permitted to direct market that person. The net effect of this provision is that organisations that conduct regular direct marketing campaigns need only screen their lists against the TPS and FPS on a monthly basis.

3.37 Regulation 20 (in relation to fax marketing) and Regulation 21 (in relation to telephone marketing) clarify that registration with the FPS and TPS does not override any opt-in or opt-out based permissions given to an organisation by a particular marketing prospect. For example, I have registered at home with the Telephone Preference Service. If I take out insurance and do not tick the direct marketing opt-out box, then the insurance company will be entitled to telephone me at home for direct marketing purposes notwithstanding that I have registered with the TPS. I am, however, entitled to give a subsequent opt-out to my insurance company under Regulation 21 (5).

Information Requirements (Regulations 23 & 24)

3.38 Regulation 24 requires specified information to be provided with direct marketing sent over a public electronic communications service. Where an organisation makes a direct marketing call by telephone, then it must provide its name. In addition, if the person called so requests, it must provide details either of its address or a freephone number at which the organisation can be reached free of charge. All of this information must be provided when direct marketing is sent by fax or via an automated calling system.

3.39 In the case of direct marketing by e-mail then there is a prohibition on disguising the identity of the sender in Reg23 (a). Organisations are also required to include a valid unsubscribe address under Reg 23 (b). Reg 23 prohibits the transmission of direct marketing e-mails:

"where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided".

@ Ruth Boardman 2004
The moral rights of the author have been asserted
Database right The Centre for International Law (maker)
3.40 The obligation to provide these identification details apply equally to SMS marketing. The Guidance states (at page 22) that despite the practical limitations imposed by 160 characters marketers must comply with the Regulations, either by providing information before the message is sent (in an advert or on a web site, for example) or in the message itself. If the recipient has clearly consented, the Commissioner considers that a suppression address maybe provided with 18 characters, as in the Guidance example of “PJLTDPOBox97SK95AF”. If relying on the soft-opt in, however, the obligation to provide a simple means of refusing further marketing with every message may require the use of up to 40 or more characters. The example provided in the Guidance is as follows: “PJLTDPOBox97SK95AF.2STOPMSGSTXT’SSTOP’TO (then add 5 digit short code)”.

Consent

3.41 The E-Privacy Regulations require notice of consent for e-mail marketing to individual subscribers, fax marketing to individual subscribers, use of automatic calling systems and use of traffic/location data for marketing/value added services.

3.42 As would be expected, the ICO’s Guidance reiterates the Commissioner’s general view on consent (e.g. the need for it to be specific, informed and freely given). In addition, the Guidance looks at the user/subscriber’s ability to revoke consent. The E-Privacy Regulations talk about consent being given “for the time being”. The Guidance (at page 5) notes that this phrase does not mean that consent only lasts for a finite period of time. Instead, once consent has been given it will remain valid until the individual has objected or there are other grounds for believing that the individual no longer wishes to receive marketing messages. Conversely, where an individual has objected to receiving direct marketing for the time being then this objection stands unless and until the individual indicates that they have changed their mind.

Who has authority to give consent?

3.43 The Guidance also addresses the rather more difficult issue as to who has authority to give consent. In some cases there is potential for confusion here. For example, if an organisation wishes to make direct marketing calls by telephone, does it need to consider the consent/objections of the subscriber (i.e. the member of the household who has the contract with the telecoms service provider or, if it wishes to speak to someone other than the subscriber, of that specific person? The Guidance works through this in quite some detail. The conclusions are as follows:

- it is the subscriber who has the right to register with the Telephone Preference Service;
- the subscriber has a general right to object to direct marketing being carried out using his line (not considered in the Guidance);
- individuals have rights to object under the Data Protection Act; individuals can, effectively, override other wishes of the subscriber if they request organisations to contact them – i.e. if they solicit marketing material by telephone. (This is on the basis that the right to object and the TPS arrangements only apply to unsolicited marketing calls).
3.44 The Guidance also considers the situation of partnerships where there is also some scope for confusion as to who must give consent. (Is it the partnership or the specific person at the partnership to whom marketing material is being sent?) Here, the Guidance concludes (page 30) that it is reasonable for the wishes of the partnership to prevail over the wishes of any individual employee. The Guidance also concludes that the consent of one person at the partnership to receive marketing cannot be taken as consent for everybody at the partnership to receive direct marketing (unless, presumably, the consent is specifically given on behalf of the whole partnership).

4. SERVICE PROVIDER SPECIFIC PROVISIONS

Traffic, billing and location data (Regs 7, 8 and 14)

4.1 Like the earlier Regulations, the E-Privacy Regulations contain a number of provisions that are of specific application to service providers. In large measure these re-state the earlier Regulations. The main changes are the inclusion of specific provisions relating to location data and new protections for subscribers in relation to reverse-searchable directories. As with the rest of the E-Privacy Regulations, these provisions now apply to all electronic communications service providers i.e. they are not specific to telecommunications service providers.

4.2 Direct marketers need to be aware of the provisions in the E-Privacy Regulations restricting the use of traffic and location data.

4.3 Traffic data is defined as:

“data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication” (Reg 2 (1)).

Whereas the Telecoms Privacy Regulations distinguished between traffic and billing data, the E-Privacy Regulations have combined these provisions.

4.4 A bill/billing is defined as “invoice, account, statement” (Reg 2 (1)).

4.5 Location data is defined as:

“data processed in an electronic communications network indicating the geographical positions of the terminal equipment of a user of a public electronic communications service, including data relating to:

● the latitude, longitude or altitude of the terminal equipment,
● the direction of travel of the user, or
● the time the location information was recorded.” (Reg 2 (1)).

4.6 A value added service is defined as a “service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing in respect of that communication”.

@ Ruth Boardman 2004
The moral rights of the author have been asserted
Database right The Centre for International Law (maker)
4.7 The E-Privacy Regulations provide that traffic data must be erased or anonymised when it is no longer required for transmission unless it is being processed for certain specified purposes (Reg 7 (1)). These are:

- billing/traffic management
- customer enquiries
- prevention or detection of fraud
- marketing of electronic communications services, provided that the subscriber or user has consented
- value added services, again providing the subscriber or user has consented.

4.8 In respect of itemised bills, a subscriber can require its bills to be non-itemised (Reg 9). In addition OFCOM is to consider the privacy issues relating to itemised bills and attempts to reconcile the rights of subscribers receiving itemised bills with the rights to privacy of calling users and call subscribers. This is, for example, particularly an issue with mobile phone users having access to work mobile phones.

4.9 Location data is specifically stated not to include traffic data. This data may only be processed where it is anonymised or it is necessary for provision of value added services and the user or subscriber has consented (Reg 14).

4.10 As we have seen, the reference to consent comes up in relation to both traffic data and location data. There are some similarities in the provisions relating to consent. The Regulations make it clear that consent can be withdraw at any time including when a user or subscriber connects to the public electronic communications network. The ability to withdraw consent must be via a simple means and free of charge. In addition, consent must be informed. This is not a surprise given that the general Data Protection Directive states that consent must be specific, freely given and informed. In the case of location data and traffic data this means providing information on what types of data will be processed, for what purpose and whether any third parties would be involved.

4.11 There are limitations on the processing which may be carried out. Processing may only be carried out by a public communications provider or a person acting under its authority. Similarly in respect of value added services the processing may be carried out by a value added services provider or a person acting under his authority.

4.12 Finally, the Regulations try to limit the processing of location and traffic data to that which is necessary or required for the specified purpose.

4.13 There is potential under the Regulations for confusion where there are shared accounts. For example, where there is a corporate subscriber and an individual user (e.g. a work mobile phone) which consent will take precedence? Equally where there are shared phones with several users (e.g. a family phone held under the name of one parent but used by the whole family) (see section 6.3, below).

4.14 There is a question which remains from both the Directive and the E-Privacy Regulations as to whether in respect of location data other than traffic data the subscriber or user must have the possibility of refusing processing both on connection and for each individual transmission of a communication, or if they only need to be offered one or the other means of temporarily refusing.
5. COOKIES (Reg 6)

What is a cookie?

5.1 A cookie is merely a small file of letters and numbers that act as an identifier. They allow the website server that sent the cookie to recognise the user when s/he returns to the site, or browses from page to page. The numbers identify the name of the server that sent the cookie, the lifetime of the cookie and, possibly, other information such as the time the cookie was placed. A cookie typically looks like this:

CFGLOBALS
HITCOUNT%3D168%23LASTVISIT%3D2003%2D06%2D10+11%3A31%3A38
%27%7D%23TIMECREATED%3D2002%2D08%2D05+10%3A58%3A19%27%7D%23
www.twobirds.com/
1536
3546759168
32088942
3714238208
29568827
*
CFID
513752
www.twobirds.com/
1536
3546759168
32088942
2326244048
29506662
*
CFTOKEN
80215158
www.twobirds.com/
1536
3546759168
32088942
2326844048
29506662
*

5.2 Cookies are primarily used to allow websites to be customised, as they allow the website’s server to recognise that it is the same user returning to it. So, for example, if you have previously visited a travel website and booked tickets to Paris, when you return to the site the server may customise the site with a message offering flights to other European cities that the site owner thinks are likely to be of interest. This potential to identify users can also be misused – a well known on-line retailer used cookies to allow it to discriminate between existing and new users of its service, so as to offer differential pricing.

@ Ruth Boardman 2004
The moral rights of the author have been asserted
Database right The Centre for International Law (maker)
What do the Regulations say?

5.3 Reg 6 (1) provides as follows:

“... a person shall not use an electronic communications network to store information [i.e. plant a cookie], or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met”.

5.4 Reg 6(2) states that:

“The requirements are that the subscriber or user of that terminal equipment –

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) is given the opportunity to refuse the storage of or access to that information”.

5.5 At first sight, it is not apparent that Reg 6 is intended to cover cookies. However, this is clear from the E-Privacy Directive, recital 24 of which specifically refers to cookies, spyware, web bugs and other hidden identifiers.

5.6 The effect of Reg 6, therefore, is to prohibit the use of cookies unless an organisation using a cookie provides information about the cookie and gives a subscriber or user the opportunity to reject the cookie before it is placed. It is already commonplace for websites to include information about cookies in their privacy policies. The information obligations, therefore, should not be particularly onerous. It may be more difficult for organisations to comply with the second requirement – that is to offer an opportunity to reject the cookie.

5.7 The DTI’s published response to the consultation exercise that preceded the E-Privacy Regulations makes clear that the DTI wished to be as un-prescriptive as possible about the ways in which organisations comply with the information and rejection provisions. For example, one possibility that was mentioned in the DTI’s consultation document was that organisations could include information in their cookie policies explaining how users could configure their browsers so as to reject cookies. (For example, some versions of Internet Explorer allow you to reject cookies). The Information Commissioner’s Guidance is not prescriptive either but stresses the importance of providing users with information that is sufficiently full and intelligible to enable them to understand the consequences of allowing a cookie to be stored and what the information collected will be used for, should they wish to accept the cookie (page 5).

5.8 Anyone who has followed the legislative process of the E-Privacy Directive may recall that there was a certain degree of controversy as to whether or not the information requirements would require organisations to use pop-up boxes to alert users that a cookie was going to be placed. This suggestion arose out of the Common Position adopted by the European Council on 28 January 2002, which stated that subscribers and users must receive information “in advance” about cookies. The direct marketing industry lobbied extensively against this – on the grounds that this would be extremely disruptive for users. The final text of the Directive omits this requirement as do the E-Privacy Regulations. The existing guidance from the Office of the Information Commissioner on
this issue (Website Frequently Asked Questions, 26 June 2001, FAQ 6) is still valid. This is that data controllers could either provide the cookie statement via a pop-up box or in the website’s privacy statement – provided this contained some clear notice that tracking technology would be used. In line with general data protection requirements, any privacy policy must be drawn to users’ attention before personal data are collected. This is reiterated in an on-line context in guidance given by the Commission working party responsible for data protection (The Article 29 Data Protection Working Party) which states that individuals must be alerted to this information when personal data are collected (Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, 17 May 2001, page 6).

Exceptions

5.9 There are a number of exceptions to the information and rejection provisions. Regulation 6 (4) provides that these obligations:

“shall not apply to the technical storage of, or access to, information –

(a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or

(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user”.

5.10 The Guidance has addressed the meaning of the term “strictly necessary” (on page 6), stating that the cookie should be essential rather than being merely necessary in order for the exemption in Regulation 6(4) to apply. It is further restricted to what is essential to provide the service that the user has requested, as opposed to essential for any other uses that the service provider might wish to make of that data. The user must in any case be told that the cookie is necessary so that the user may decide whether to proceed.

5.11 There is also some interesting comment in the Guidance as to the impact of the information/rejection provisions on websites where cookies can be planted by third parties, as opposed to the website operator. The most common example of this would be where a website includes third party adverts which, in turn, plant cookies on the user’s terminal. The Guidance states that the organisation to whom the site primarily refers must alert users to the fact that third party advertisers operate cookies. The third party advertiser also then has to comply with the information obligations, presumably by advance notice to users where technically possible. This requirement may prove disruptive to online advertising if followed.

5.12 In addition to the exceptions at Reg 6 (4), Reg 6 (3) makes clear that the information/rejection requirements can be complied with once only and that this will then be valid for subsequent visits by the user to the website. Reg 6 (3) provides that:

“Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of (2) are met in respect of the initial use”.

@ Ruth Boardman 2004
The moral rights of the author have been asserted
Database right The Centre for International Law (maker)
5.13 Recital 25 of the E-Privacy Directive makes this provision somewhat clearer. This states that the information/rejection provisions may be offered on a one-off basis covering the initial collection and any further use of the cookie or similar devices during subsequent connections.

5.14 Organisations may also choose to make provision of a service conditional upon the user accepting the cookie – i.e. the E-Privacy Regulations do not override contracts in this instance (note however, Regulation 27 which prohibits service providers and network providers from contracting out of the Regulations). This is not referred to in the Regulations. However, this is expressly set out in the E-Privacy Directive. Recital 25 of this states that services can be conditional on acceptance of a cookie if the cookie is used for a legitimate purpose. Organisations adopting this approach would, however, need to ensure that the website terms and conditions were brought to the user’s attention before or at the time that any personal data were collected in order to comply with general data protection requirements.

5.15 Careful readers of the E-Privacy Regulations may note that there is potential for conflict between the rights of subscribers and the rights of users (that is between the person who enters into the contract with the ISP and the person who actually uses an online service). This is because the E-Provacu Regulations provide that the information/rejection provisions are met where “the subscriber or user of that terminal equipment” is provided with information and the opportunity to reject i.e. the E-Privacy Regulations do not specify whose wishes are to take precedence where they are in conflict. An organisation need not, therefore, provide information and an opportunity to reject cookies to each subsequent person that uses its service from the same terminal. It is sufficient if the subscriber gives consent initially. This is likely to be of use to organisations making available internet services to corporates, as there is the potential to provide the information and rejection provisions in the original terms and conditions accepted by the business, as opposed to having to provide this when individual employees access the service. The Guidance (at page 7) provides the example of an employer, as subscriber, being reasonably entitled to have its wishes take precedence in the situation where it is providing the terminal to the employee at work and where the performance of certain tasks would require the use of a cookie. This is qualified by the advice that if such a cookie involved the unwarranted collection of personal data from the employee then the employer’s wish to accept the cookie would be unlikely to prevail over the employee’s rights as a data subject. In the consultation exercise, the DTI invited comments as to whether this arrangement would be problematic. Its conclusion in the response to consultation (Implementation of the Directive on Privacy and Electronic Communications: Government’s Response to Consultation, 18 September 2003, para 13) is that there are likely to be very limited cases in which there would be conflicts between subscribers and user rights. However, the DTI does note that it has not ruled out taking further action in this area in the future should this prove necessary.

6. CONSEQUENCES OF NON-COMPLIANCE

6.1 Individuals may, in probably quite limited circumstances, seek compensation if an organisation breaches the E-Privacy Regulations. Regulation 30 provides that a person who suffers “damage” by reason of any contravention of the Regulations may bring proceedings for compensation from that other person. As damage is interpreted as meaning physical or economic loss, it is probably only in relatively limited situations that
a person who has received unwanted direct marketing would be able to rely on this provision.

6.2 There may be more scope for competitors of organisations to bring claims for compensation under Regulation 30. For example, an organisation that has complied with the Regulations may be able to show that it has lost sales to an organisation that has not complied. Regulation 30 is not restricted to persons receiving unsolicited commercial communications. Instead it is open to any “person” who suffers damage through breach of the Regulations to bring proceedings. Regulation 30 may also be used if an organisation incurs losses because of poor network security. The organisation incurring loss could bring proceedings directly against the service provider for breach of the security obligations at Regulation 5.

6.3 In the event of proceedings being brought under Regulation 30 (1), Regulation 30 (2) provides that it is a defence to prove that such care has been taken as, in all the circumstances, was reasonably required to comply with the relevant requirement.

6.4 The E-Privacy Regulations modify the Data Protection Act so as to grant the Information Commissioner powers to enforce the Regulations. So, the usual powers of the Commissioner to issue information and enforcement notices and, if necessary, to obtain a search and seize warrant are applied to these Regulations.

6.5 Regulation 32 provides that the Commissioner may take action either on his own initiative or as the result of a complaint from a person affected by a breach of the Regulations or a complaint made by OFCOM. OFCOM is also tasked, under Regulation 33, with providing technical advice to the Commissioner in response to any reasonable request made by the Commissioner in connection with his enforcement functions.

6.6 The DTI did invite responses as to whether the Commissioner’s enforcement powers should be strengthened. Some responses to the consultation exercise argued that the Commissioner should be given powers to issue “stop now” orders or powers to levy direct fines. However, in the end, these provisions were not adopted. The DTI has, however, committed to holding further discussions on enforcement with service providers and other stakeholders. One of the items on the agenda for these discussions is the question as to whether or not service providers should be mandated to disclose the identity of organisations breaching the Regulations.