Legal & Regulatory Update

Shelagh Gaskill

is a partner in the Information and Technology Department at Masons. She specialises in information law which relates to the commercial exploitation of data of all types, including their acquisition, sale and exchange, as well as the legal aspects of the establishment and design of databases, worldwide dataflows, data protection and privacy laws in the UK, Europe and third world countries.

Adrian Hackett

is a trainee solicitor in the Information and Technology Group at Masons and is currently working on a number of regulatory compliance issues. He has an interest in corporate tax and funding, particularly in relation to e-commerce.

Spam and text messaging

E-mail and text message marketing

Shelagh Gaskill and Adrian Hackett

Date received: 11 June 2001

Introduction

Digital mobile communications networks and the Internet now enable the delivery of a wide range of electronic communications services.

Reminders may be sent by e-mail when theatre tickets come on sale, and global positioning systems allow advertisers to use location-based advertisements to market the products and services of every shop that an individual walks past. In addition, 'push technology' now allows retailers to send an alert every time a new product is available and for mobile telephone users to place an order at the push of a button. Should the UK or EU follow the lead of Japan, telephone users will also be given the opportunity to finance transactions made via their mobile telephones by adding the purchase price to their telephone bill.

The EU Commission has expressed its intention not to stifle the development of this technology. However, it also recognises the potential impact that it may have on the privacy of individuals. Almost everyone with a private e-mail account undergoes the irritating and time-consuming task of opening and deleting unsolicited e-mails, or 'spam' each time they open up their inbox. Marketing information sent direct to a mobile telephone in the form of a text message may also be intrusive. The EU Commission has therefore enacted new legislation which both enables and regulates the use of electronic communications services.

Unsolicited communications

The EU directive concerning the processing of personal data and the protection of privacy in the telecommunications sector (97/66/EC) (the Telecommunications Directive) imposes restrictions on the use of a public telecommunications network for the unsolicited communication of material for the purpose of direct marketing. Prior consent is required for the communication to individuals of such material by automated calling machine and fax, and member states must take appropriate measures to ensure that unsolicited direct marketing calls by other means are not allowed either without the prior consent of subscribers or in respect of subscribers who do not wish to receive these calls. The choice between these two options may be determined by national legislation. These provisions are enacted into UK law by the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1999 (the Telecommunications Regulations).

Shelagh Gaskill and
Adrian Hackett
Masons, Springfield House,
76 Wellington Street,
Leeds LS1 2AY, UK
Tel: +44 (0) 113 233 8905

E-mail

What is a “call”?

No definition of the term ‘call’ is given in the Telecommunications Directive and, although some member states have included provisions restricting unsolicited e-mail marketing, the Telecommunications Regulations, as well as the legislation of a number of other member states, have interpreted the term ‘call’ in a narrow sense to protect subscribers only from unsolicited telephone calls and not from e-mail.

This problem is recognised in the proposed directive on the processing of personal data and the protection of privacy in the electronic communications sector (500PC0385) (the E-Communications Directive), which is intended to replace the Telecommunications Directive. The E-Communications Directive contains a provision which requires the consent of any individual to be obtained before direct marketing material is sent to them by automated calling machines, fax or e-mail. This provision must be enacted into EU member state national legislation by 31 December 2001.

Text messaging

It is also not clear from the Telecommunications Regulations whether the protection from telephone marketing communications applies regardless of the type of data which are transmitted or whether the restrictions apply solely to voice telephony. The Telecommunications Regulations merely state that a caller may not make a telephone marketing call to an individual who has either notified the caller that he objects to such calls or if the number has been registered with the Telephone Preference Service.

The E-Communications Directive requires legislation to be enacted which clarifies this position. It provides that member states must take measures to ensure that a caller may not make an unsolicited communication to an individual, by means other than an automatic calling machine, fax or e-mail, if either that individual has not given his prior consent or the individual has indicated that he does not wish to receive such communications. The choice between these options may be determined by the member state.

“Call” now replaced by “communication”

The term ‘call’ has therefore been replaced by the term ‘communication’ which the preamble to the E-Communications Directive states is intended to apply to all new forms of communication, as well as to voice telephony. Although not expressly stated, other new forms of communication are clearly intended to include text messages.

E-mail and text message marketing to businesses

The E-Communications Directive provides that member states must also enact applicable legislation to protect the legitimate interests of companies from all unsolicited communications. Measures must therefore be enacted to restrict both e-mail and text message marketing, although it is not clear whether these measures will be opt in or opt out.

Traffic data

Traffic data are data processed in the course of, or for the purpose of, the transmission of a communication and are necessary for the purpose of

billing and interconnection services. Under the Telecommunications Regulations the use of traffic data is restricted to:

- the management of billing or traffic
- customer enquiries
- the prevention and detection of fraud
- the marketing of any telecommunications services provided by the service provider.

EU encouraged value-added services

The European Commission considers this to be too narrow. Traffic data may also be used to provide what has been described as ‘value-added services’ and the Commission is keen not to stifle the development of such services. The full scope of value-added services is not defined in the E-Communications Directive, although they include such services as the provision of individual traffic information and guidance to motorists.

However, given the potential intrusion into personal privacy to which the use of such data may give rise, a number of restrictions are also imposed. In particular, unless the subscriber has consented to any further processing for the purposes of providing value-added services, traffic data may be stored only to the extent necessary for the purpose of billing and for interconnection services and only for the period during which the bill may be lawfully challenged or the payment pursued.

Mobile phones locate users to within 15 metres

Location data

Location data give the geographical position of a mobile telephone used on a digital mobile network. Such data are necessary to enable the transmission of communications and are useful for emergency services to be able to send assistance or rescue teams to mobile users who may not be able to describe where they are. Such data may also be used for the provision of value-added services.

As with traffic data, the processing of location data is also considered to pose a risk to personal privacy, and the E-Communications Directive places a number of restrictions on their use. Location data may only be processed if they are made anonymous, or with the consent of the subscriber, and then only to the extent and duration necessary for the provision of the service. Even in cases where subscribers have given their consent, they should have a simple means to deny temporarily the processing, free of charge. Service providers must also inform users, before obtaining consent, of the type of location data to be processed, the purposes and duration of processing and any disclosures to third parties.

Proposed EU directive on the distance selling of consumer financial services

The proposed EU directive on the distance selling of consumer financial services (Distance Selling of Financial Services Directive) imposes restrictions on the use of distance communication for the unsolicited transmission of material for the purpose of direct marketing of financial services to consumers. Communication by any means other than by

automated calling system or fax is only allowed for the distance marketing of financial products if:

- the caller has obtained the prior consent of the consumer; or
- the consumer has not raised an objection to their use for this purpose.

The choice between these options is at the discretion of the member state.

The Data Protection Act 1998

Compliance with the Telecommunications Regulations, the E-Communications Directive and the proposed EU Distance Selling of Financial Services Directive does not remove the necessity also to comply with the Data Protection Act 1998 ('the 1998 Act').

Personal data

The 1998 Act imposes restrictions on the use of personal data, whether for direct marketing purposes or otherwise, by a data controller. E-mail or text message marketing therefore only fall within the scope of the 1998 Act if an e-mail address or mobile telephone number may be classified as personal data.

Can you be identified from your e-mail address or mobile phone number?

E-mail address as personal data

The 1998 Act defines personal data as data which relate to a living individual who can be identified from those data or from those data and other data in the possession of the data controller. This applies to an e-mail address in cases where the e-mail address serves as an aide memoire to the identity of its owner, for example, fred.bloggs@ici.com or fb@ici.co.uk. In these addresses a corporate domain name is being used and, using any available directory, Fred Bloggs's whereabouts could be traced.

If the address were simply fred@ic24.net, all that is known about the individual is that Fred is his Christian name and IC24 is his e-mail service provider. This information does not therefore of itself provide sufficient information from which Fred can be identified.

However, since data are also personal data if an individual can be identified from those data and other data in the possession of the data controller, if an individual can be identified from his e-mail address and any associated documentation or behaviour, this address will constitute personal data. This might occur if, for example, the identity is revealed from the content of the e-mail or any electronic record built up about that person through the use of 'cookies', registration forms or traffic data.

In her advice of 14 December 2000, the Information Commissioner further stated that an e-mail address is personal data even if it is not possible to locate an individual in the physical world from that address, or from that address and any other information in the possession of the data controller. It is sufficient that tracking technology is able to build up a profile about an individual from his e-mail address and that this can uniquely locate him in the online world.

What can direct marketers do?

Mobile telephone numbers as personal data

Mobile telephone numbers are personal data if an individual can be identified from the number or from the number and other data in the possession of the data controller. A mobile telephone number would therefore be personal data if any associated material could identify the user of the telephone.

Since global positioning systems can locate the telephone to within 15 metres and a record of all calls and transactions carried out using the telephone may be made, a detailed profile of the owner of a mobile telephone number may be established which may allow an individual to be identified. A mobile telephone number may therefore also be classified as personal data.

Fair and lawful processing

The 1998 Act requires a direct marketer, as data controller, to process any personal data, including e-mail addresses and mobile telephone numbers, fairly and lawfully. This principle requires the processing of personal data to be justified under one of the six grounds in Schedule 2 of the 1998 Act. The Schedule 2 grounds which are most appropriate to a direct marketer are that he has obtained the consent of the data subject or that direct marketing is in the legitimate interests of the data controller, as it is unlikely to cause prejudice to data subjects since they have an absolute right to stop the marketing.

If a customer profile has been built up through the use of traffic or location data which contain sensitive personal data, for example, data which indicate an individual's racial or ethnic origin, political opinions, physical or mental health, sexual life or the commission of an offence, then a Schedule 3 condition must also be found. The only appropriate Schedule 3 ground for direct marketing is explicit consent.

The data controller is also required to serve a data protection notice on the data subject. This must describe the identity of the data controller, the purposes for the processing, the recipients of the data, their purposes and any other information that is necessary to make the processing fair. This includes the methods and means of communication, for example, contact by mail, telephone, fax or e-mail. Most data protection notices do not include text messaging as a means by which direct marketing may be sent although, given its intrusive nature, it too may have to be included. The notice should also include the data types and extent to which traffic or location data are processed.

Right to object to direct marketing

The 1998 Act grants an individual an absolute right to object to the use of his personal data for direct marketing purposes. This applies to all forms of direct marketing, including e-mail and text messaging.

Summary

Table 1 summarises the provisions which, when enacted, will regulate how direct marketers are able to use e-mail and text messaging to send marketing material to individuals and businesses.

Table 1: Use of e-mail and text messaging for marketing

	E-mail		Text messaging	
	Not using traffic data and/or location data	Using traffic data and/or location data	Not using traffic data and/or location data	Using traffic data and/or location data
Individual	Opt in	Opt in	Opt in/opt out	Opt in
Company	Opt in/opt out	Opt in	Opt in/opt out	Opt in

The requirement for prior consent contained in the E-Communications Directive is likely to be reflected in the 1998 Act as a justification to the processing of sensitive personal data if the use of traffic or location data involves processing sensitive personal data.

In conclusion, e-mail and text messaging services will be of enormous value to users — for example, information alerting users about a traffic jam a few miles ahead on the motorway or reminders that tickets which the user's profile suggests will be of interest to him are to go on sale the next day. The revised EU legislative framework relaxes previous restrictions on the availability of these services. In doing so, however, it also recognises that not all individuals want all the services on offer and that it is essential that their provision is consensual.