BEIJING
BRUSSELS
CHICAGO
DALLAS
GENEVA
HONG KONG
LONDON
LOS ANGELES
NEW YORK
SAN FRANCISCO
SHANGHAI
SINGAPORE
TOKYO
WASHINGTON, DC

SIDLEY AUSTIN BROWN & WOOD
AND AFFILIATED PARTNERSHIPS

NEW LEGAL REQUIREMENTS IN ONLINE MARKETING

December 2003

BACKGROUND

The online environment has led to an increased level of sophistication in marketing activities carried out by businesses. The technology exists for businesses to develop very accurate profiles of the interests and preferences of their users. This information can be exploited to identify potential customers of their products and services. Businesses can then target large numbers of consumers efficiently and cost-effectively in their marketing campaigns.

The ease with which business can approach individuals and collect data about them has led to concerns about privacy. Individuals' rights to privacy are laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms. A raft of legislation has been introduced by Brussels to harmonise privacy rules across the EU, to protect the interests of the consumer and so ultimately build up confidence regarding electronic commerce.

This paper focuses on the two strands of the privacy debate: firstly, the practice of soliciting business through unsolicited commercial communications (that is communications which have not been requested by the recipient) and, secondly, the extent to which personal data may be collected by invisible tracking devices and processed and used for commercial purposes. This paper does not specifically consider the nature of the notifications that organisations engaged in direct marketing are required to provide to individuals from whom they collect personal information.

GENERAL REGULATORY REGIME

It is an objective of the EU to harmonise the laws of the Member States on privacy. However, the EU has adopted a piecemeal approach, with several Directives now governing this area of law.

THE DATA PROTECTION DIRECTIVE 1995/46

The Data Protection Directive provides the primary legislation through which direct marketing activities are regulated, and the provisions of this Directive generally take priority over the provisions of the other Directives. The Data Protection Directive regulates the collection and processing of personal data for business purposes. The concept of 'processing' is so broad that it effectively includes anything at all, even the mere storage of personal data. The Data Protection Directive is implemented in the UK by the Data Protection Act 1998.

THE E-COMMERCE DIRECTIVE 2000/31

This Directive applies to information society services (ISS), namely services normally provided for remuneration at a distance by electronic means and at the individual request of the recipient of the service. The Directive specifically states that ISS include commercial communications, which are in turn defined as any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial activity or exercising a regulated profession. Recipients may be natural or legal persons who, for professional ends or otherwise, use an information society service, in particular for the purposes of seeking information or making it accessible. The E-Commerce Directive is implemented in the UK by the Electronic Commerce (EC Directive) Regulations 2002.

THE DISTANCE SELLING DIRECTIVE 1997/7

This Directive applies to distance communications, that is, any means which may be used for the conclusion of a contract for goods or services (other than financial services) between a supplier and a consumer, which does not involve the simultaneous physical presence of the parties. A consumer means any natural person who, when entering into a distance contract, is acting for purposes outside his trade, business or profession. This Directive is implemented in the UK by the Consumer Protection (Distance Selling) Regulations 2000.

THE DISTANCE MARKETING OF FINANCIAL SERVICES DIRECTIVE 2002/65

This Directive applies to distance communications, that is, any means which may be used for the conclusion of a contract for financial services between a supplier and a consumer, which does not involve the simultaneous physical presence of the parties. A consumer means any natural person who, when entering into a distance contract, is acting for purposes outside his trade, business or profession. Member States are required to implement this Directive before 9 October 2004. There is currently no draft implementing legislation for the UK.

THE PRIVACY & ELECTRONIC COMMUNICATIONS DIRECTIVE 2002/58

This Directive aims to use technology neutral language to cover both existing means of communication and other methods that may be developed in the future, for the processing of personal data of subscribers or users in connection with the provision of publicly available electronic communications services in public communications networks. The Directive focuses on the subscribers to, and users of, public communications networks, who may be natural or legal persons (users are limited to natural persons). Member States are required to implement this Directive before 31 October 2003. The UK implementing regulations, the Privacy & Electronic Communications (EC Directive) Regulations 2003 (the "Privacy & Electronic Communication Regulations") were laid before Parliament on 18 September 2003 and will come into force on 11 December 2003.

UNSOLICITED COMMERCIAL COMMUNICATIONS

Up until fairly recently, there was not any legislation which specifically dealt with unsolicited commercial communications. Unsolicited promotions, regardless of the form of medium used, were simply subject to the general principles of the Data Protection Directive. However, it has been a recent ambition of the EC Commission, firstly, to distinguish between the different types of medium by which unsolicited commercial communications may be sent and, secondly, to harmonise the laws of the Member State in relation to the use of unsolicited commercial communications sent to individuals in all forms of medium. The EC Commission has achieved its aims by introducing the various Directives pursuant to which the Member States are required to adopt the specified minimum standards for the protection of individuals.

DIRECT MARKETING GENERALLY

The first principle of the Data Protection Directive requires that personal data is processed fairly and lawfully. For information to be processed fairly and lawfully (i) there must be a legitimate condition for processing and (ii) the individual to whom the information relates must be provided with certain "Fair Collection Information". In the context of marketing, the only legitimate conditions which are likely to be relevant are as follows:

- The individual concerned has consented to the use of his data for marketing purposes.
- It is in the legitimate interests of the data controller to use the individual's data for marketing and such use does not unfairly prejudice the rights and freedoms of the individual.

Many businesses wish to avoid the issue of consent and instead rely on the legitimate interests condition. Indeed, this approach is promoted by the Direct Marketing Association. However, it could be argued that an individual's right not to be targeted with unsolicited promotions is greater than a business's right to advertise its goods or services. Whilst there may be some merit in this legitimising condition for existing customers (at least as far as marketing of similar products or services as those which form the basis of the existing relationship between the business and its customer are concerned), it is unlikely that this condition will be available for marketing to prospects.

So in the context of direct marketing to persons who are not existing customers, the better view is that consent should be obtained. However, businesses should be aware that consent is an inherently fragile method of legitimising personal data processing, in that it can be withdrawn by an individual at any time.

CONSENT

The Data Protection Directive does not state whether consent should be obtained using the opt-in or opt-out approach. The concept of "consent" was originally defined under the Data Protection Directive[1] as "any freely given specific and informed indication of the individual's wishes by which the individual signifies his agreement to personal data relating to him being processed". The word "signifies" suggests that there should be some form of active communication from the individual to the organisation, and logically leads to the conclusion that inaction on the part of the individual is not sufficient to constitute consent. Nonetheless, in the UK "consent" under the Data Protection Directive for the purposes of direct marketing has been interpreted such that it may be obtained on either an 'opt in' or an 'opt out' basis.

OPT-IN

Opt-in refers to a system whereby businesses may not send unsolicited commercial communications unless they have obtained the prior express consent of the individual to whom the communication is to be sent. In the context of the Privacy & Electronic Communications Directive, the Recitals provide some guidance in that "consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website".

[1] Article 2(h) of the Data Protection Directive

OPT-OUT

Opt-out refers to a system whereby businesses may not send unsolicited commercial communications to individuals who have either previously notified the business concerned that they do not wish to receive such forms of communication or who have registered their objection on a national opt-out list. Businesses are under a duty to consult the relevant opt-out lists.

In the UK the opt-out registers, which comprise the Fax Preference List, Telephone Preference List, Mailing Preference List and E-Mail Preference List have received government approval. They are operated by the Direct Marketing Authority (DMA) on behalf of OFTEL. Members who subscribe to the DMA's rules are required to clean their marketing lists against these opt-out registers, although this is not a legal requirement. Nonetheless, the Information Commissioner encourages cleaning against these lists, and it is possible that, if he were to find an organisation to be in breach of its data protection obligations generally, he would require that organisation by order to clean against these preference lists in the future.

Although businesses are unable to register on the opt-out lists, they are offered protection under the Telecommunications Act 1984, which provides that anyone running a telecommunications system in the UK under a class licence is required to cease using the telecommunications system to make calls to sell their products on receipt of a written request from a subscriber to do so. If a corporate subscriber continues to receive calls from the offending party, the subscriber can ask OFTEL to enforce the legislation.

Even if an opt-out approach is permitted for unsolicited commercial communications sent by a particular medium, where the data collected includes sensitive data, then only an opt-in approach will be sufficient. Sensitive data can include information as to an individual's race, ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life or criminal offences or proceedings.

RIGHT TO OBJECT TO DIRECT MARKETING PURPOSES

In addition, the Data Protection Directive specifically gives individuals the right to object (opt-out), free of charge, to their personal data being processed for direct marketing purposes or to their personal data being disclosed for the first time to third parties for the purposes of direct marketing[2]. The Data Protection Act 1998[3] states that an individual is entitled, at any time upon written notice, to require a data controller to cease or not begin, using their personal data for direct marketing purposes. "Direct marketing" is defined as the communication by any means, of any advertising or marketing material which is directed to particular individuals. This includes sending faxes, personally addressed mail, e-mails or mobile text messaging (SMS) to individuals and calling individuals. It also includes the use of on-line advertising which has been specifically targeted to a particular individual, such as banner ads on websites that appear only to certain specifically chosen browsers.

[2] Article 14(b) of the Data Protection Directive
[3] Section 11(1) of the Data Protection Act 1998

FAX AND AUTOMATED CALLING SYSTEMS

The practice of using fax and automatic calling machines[4] for marketing purposes is regarded as particularly invasive of individuals' privacy by the EC Commission, and for this reason is strictly controlled. An opt-in approach has consistently been adopted by the various Directives. The Distance Selling Directive, the Distance Marketing of Financial Services Directive, the Privacy & Electronic Communications Directive and the Telecommunications (Personal Data & Privacy) Directive all prohibit the use of automatic calling machines and fax machines for direct marketing purposes to contact individuals or consumers unless they have previously consented, regardless of whether personal data is used.

E-MAILS ('SPAM')

The ease with which e-mails may be sent to a vast number of individuals in a relatively short period of time and at very little cost to the sender, makes marketing online an attractive alternative to more traditional mediums. However, the recipients' experience is quite different. Unwanted e-mails take up space on a recipient's computer system, reducing the system's performance, and the recipient has to pay for connection time while downloading, filtering and reading the unsolicited e-mails.

As the practice of sending unsolicited promotions electronically has increased, so the EC Commission has toughened its stance towards this practice. The first of the series of Directives to specifically address the use of unsolicited commercial communications, the Distance Selling Directive, merely states that unsolicited promotions may be sent by any medium other than fax or automatic calling machine unless there is a clear objection from the consumer. Next, the Distance Marketing of Financial Services Directive introduced the option of an opt-in approach, giving Member States the choice between the opt-in and opt-out approach for unsolicited commercial communications sent by all media other than fax or automatic calling machine. The more recent Privacy & Electronic Communications Directive has introduced a requirement of prior consent.

Prior to the UK's implementation of the Electronic Communications and Privacy Directive, there has been no absolute prohibition on unsolicited electronic mails for marketing purposes, since the Telecommunications (Data Protection and Privacy) Regulations 1999 were not generally considered to apply to e-mail. Nonetheless, the Information Commissioner took the view that where a data controller processes personal data in the form of e-mails and continues to send unsolicited commercial communications to those individuals who have notified that they do not wish to receive such communications or have registered on an opt-out list, such marketing activities would involve unfair processing in breach of the Data Protection Act 1998.

The Privacy & Electronic Communications Directive prohibits the use of electronic mail to send unsolicited commercial communications to individual subscribers unless they have previously consented (subject to the exception for existing customers). Electronic mail is defined to mean "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient". "Terminal equipment" is not defined but does not appear to be restricted to PCs and so will include any mobile device designed to

[4] For example, a number may be selected at random by an automatic calling machine and, when the subscriber picks up the call, he is connected to a sales person.

retrieve and receive text messages and/or electronic mail. The Privacy & Electronic Communications Regulations remove any element of doubt on this matter by stating that "electronic mail" includes "messages sent using a short message service".

There is an exception to the requirement of prior consent for the use of unsolicited promotions by electronic mail. This allows electronic contact details collected during a previous transaction to be used for direct marketing of similar products or services by electronic mail. However, this exception is quite narrow because it is subject to the following conditions:

- The electronic contact details must have been obtained in the context of a genuine prior 'sale of a product or service'. It has therefore been questioned whether this exception would apply to electronic contact details collected as a result of customer enquiries or competitions. The Privacy & Electronic Communications Regulations extend the scope of a prior relationship to negotiations for the sale of a product or service, but do not clarify whether contact details collected from customer enquiries or competitions are included.

- Only the natural or legal person who collected the electronic contact details can use them for direct marketing. This may cause problems where marketing is carried out by a separate agency or where group companies wish to share customer data.

- The details can be only used to market 'similar' products or services – as yet there has been no guidance as to what 'similar' means in this context. Some commentators have suggested that from a strategic and operational standpoint, the elements that often determine the similarity between products or services in a business to consumer context are the use of consistent practice and branding, integrated marketing and the availability of the products or services from a single location (online and/or offline).

- The electronic contact details must have been collected in accordance with the Data Protection Directive. In other words, the data must have been collected fairly and lawfully, and the individual must have been told of the purposes for which that data might be used.

- The customer must be given the opportunity to object, free of charge, to such use of his electronic contact details, both when the data is collected and when each message is sent.

Notably, the requirement of prior consent under the Privacy & Electronic Communications Directive only applies where the subscriber is a natural person.[5] So if the subscriber is a legal entity, the opt-in regime does not apply even if the e-mail is addressed to an individual. This means that Member States may choose whether to adopt an opt-in or opt-out approach to the practice of organisations sending unsolicited marketing material to individuals in their employment environment. This position is consistent with the position laid down in the Telecom Directive.

[5] Although under the Privacy & Electronic Communications Regulations, some business subscribers, such as sole traders and partnerships (outside of Scotland) are considered as natural persons and therefore benefit from the opt-in requirement.

In any event, unsolicited commercial communications are not allowed to be sent by electronic mail unless the electronic mail clearly states the identity of the sender and an address to which the recipient may request that further communications cease[6].

Furthermore, the E-Commerce Directive requires that unsolicited commercial communications by electronic mail are clearly and unambiguously identifiable as such by the recipient as soon as they are received. However, it is still unclear what form this identification should take or whether it will be adequate to make this clear within the text of the e-mail. Unsolicited promotions by electronic mail should clearly identify on whose behalf the communication is made. Any promotional offers should be clearly identifiable as such and the conditions for participation clearly presented. Service providers which send unsolicited promotions by electronic mail should regularly consult and respect opt-out registers[7].

The Privacy & Electronic Communications Directive states that the legitimate interests of corporate subscribers in respect of unsolicited commercial communications should be sufficiently protected. Also, where businesses can register on national opt-out lists, the obligation imposed by the E-Commerce Directive on companies engaged in direct marketing to respect the wishes of natural persons registered on those lists extends to registered businesses.

MOBILE TEXT MESSAGING (SMS)

Whilst it is clear that SMS constitutes electronic mail for the purposes of the Privacy & Electronic Communications Directive, there has been no guidance on the technical status of SMS for the purposes of the various earlier Directives.

In particular, it is unclear whether the identification requirements for unsolicited electronic mail, as laid down in the E-Commerce Directive, should apply to messages sent by SMS. Although in principle these requirements are likely to apply, the DTI guidance on the implementation of the Directive makes it clear that messages sent by SMS do not fall within the definition of electronic mail. Plus, the implementing Regulations do not require service providers who send commercial communications via e-mail to consult the relevant preference service on the grounds that recipients of unsolicited commercial communications are already adequately protected under existing industry self-regulation.

If unsolicited commercial communications are sent in the form of premium-rate SMS, UK service providers should follow the Codes and Guidelines issued by the Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS), which is the telecommunications industry-funded regulatory body for all premium-rate charged telecommunications services. The ICSTIS Codes and Guidelines impose obligations on service providers to ensure that any marketing messages are legal, honest and decent, and that any premium-rate call charges which may be payable should be clearly set out. 'Unsolicited promotions' attract special rules (guideline 17), including a requirement that marketing messages sent via an automated system have the prior consent of the user. In the event of a complaint, ICSTIS will first refer non-compliant companies to the DMA and Information Commissioner, although it reserves the right to take direct action for breach of

[6] Article 13(4) of the Privacy & Electronic Communications Directive and Regulation 23 of the Privacy & Electronic Communications (EC Directive) Regulations

[7] Article 7 of the E-Commerce Directive

its Codes. Sanctions for non-compliance include fines, denial of access to the network and being blacklisted from providing such service in the future.

ALL OTHER MEDIA

In relation to unsolicited commercial communications sent by all other media, namely post and phone calls with human intervention, Member States may choose between an opt-in or opt-out approach. The Distance Selling Directive sets a minimum standard of the opt-out approach, and the Distance Marketing of Financial Services Directive and the Privacy & Electronic Communications Directive give Member States the choice between the opt-in and opt-out approach. The UK has consistently adopted an opt-out approach to direct marketing by these types of media.

SANCTIONS

Non-compliance with the rules relating to unsolicited commercial communications are likely to lead to sanctions being imposed under the Data Protection Directive or the Privacy & Electronic Communications Directive. The Data Protection Directive provides that Member States must implement enforcement mechanisms and establish sanctions for data controllers who fail to comply with their obligations under the legislation. In the UK, the Information Commissioner can issue an enforcement notice requiring an infringing data controller to comply with the Data Protection Act 1998 and, if they fail to do so, can impose unlimited fines. The Act also provides that an individual who suffers damage or distress as a result of a breach by a data controller is entitled to compensation from the data controller. In relation to direct marketing, the Act states that an individual can apply to the court for an order requiring the infringing data controller to comply with the individual's request to cease or not begin using their data for marketing. The Privacy & Electronic Communications Directive adopts the judicial remedies, liability and sanctions laid down in the Data Protection Directive.

CROSS-BORDER DIRECT MARKETING

One of the fundamental principles of the E-Commerce Directive is that online transactions will be governed by the regulatory regime of the Member State in which the supplier is established (the "country of origin" approach). However, this principle is specifically stated not apply to unsolicited commercial communications by electronic mail. This means that the rules for determining the governing law of unsolicited promotions are the same, regardless of the medium by which they are sent. The governing law should be determined by the Rome Convention[8]. The basic rule for consumer contracts is that, although the parties may choose the applicable law, this choice must not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of law in the consumer's country (generally speaking, assuming the consumer was targeted in his home country).

So, in practice a business engaged in direct marketing to individuals should carefully consider the laws of all of the Member States in which its target audience is located, since these may vary greatly. The Directives have only set out a minimum level of protection for individuals against unsolicited commercial communications: each Member State may choose to grant more protection in favour of individuals or even to introduce a level of protection for businesses from such forms of communications. Furthermore, in certain areas the Directives give Member States a choice as to whether to adopt an opt-in or opt-out approach. Member States such as Germany, Denmark and Austria tend to take a much

[8] The 1980 Rome Convention on the Law Applicable to Contractual Obligations

stricter approach to unsolicited commercial communications than Member States such as the UK and France which prefer the opt-out approach. For example, in Germany unsolicited phone calls whether or not by means of an automated calling system are completely prohibited.

The question of whether individuals have in fact given consent will be determined by the applicable national law, since to date the concept of "consent" has been subject to different interpretations by the various Member States when adopting an opt-in approach. For example, Italy has held that express consent is necessary[9], whereas Germany has held deemed consent to be sufficient[10]. The form of the opt-out registers may also differ widely between Member States as they are not actually the subject of any regulations. For example, the opt-out registers may have been approved by the Member State or they may simply be run as voluntary schemes by trade associations.

MARKET RESEARCH TOOLS

The technology used in conjunction with online communications provides many opportunities for businesses to build up usage profiles of their users. However, the EC Commission is very strongly of the opinion that terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. Personal data (as defined under the Data Protection Directive) collected on-line is protected primarily under the Data Protection Directive, as supplemented by the Privacy & Electronic Communications Directive.

DEVICES FOR COLLECTING INFORMATION ON USERS

Software programmes may be quite invasive in terms of monitoring usage and preferences of users. They can be loaded onto a user's terminal without his knowledge to gain access to information, to store hidden information or to trace the activities of the user. However, such devices can be a legitimate and useful tool, for example in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transaction.

Cookies are the most commonly known type of such devices. These are text files downloaded onto the hard drive of a user's computer when the user visits a website. Cookies enable the website to recognise repeat visitors, and can be used to build up a profile of the user's preferences. From this information, the website owner may target specific users and tailor the website to them.

The Privacy & Electronic Communications Directive provides that electronic communications networks may be used to store information or to gain access to information stored in the terminal equipment of a subscriber or user, in each case for legitimate purposes, provided, firstly, that users are given 'clear and comprehensive' information in accordance with the Data Protection Directive about the purposes of the processing and, secondly, users are given the opportunity to refuse such processing (opt-out).

[9] e.g. Article 10 of the Italian Legislative Decree No. 171 dated 13 May 1998 implementing the Telecommunications Data Protection Directive

[10] e.g. Article 89(7) of the German Federal Telecommunications Act dated 31 July 1996

So service providers will need to ensure that the necessary notification and opportunity to refuse cookies is given to users before they are placed on the terminal computer. The on-line notification may appear before data collection begins or may form part of the privacy policy. However, if the notification is provided in the privacy policy, at least some reference to the use of tracking technology should be clearly displayed to all site visitors.

The introduction of these rules is not intended to prohibit any technical storage of this information for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network or as strictly necessary to provide a service requested by the subscriber or user, provided that the information is not stored for any longer than is necessary for the transmission and for traffic management purposes.

In the UK the Information Commissioner has commented in a legal guidance note on the practice of collecting or manipulating online data:

- Cookies – Whenever an operator links a profile to a name and postal address or even an e-mail address this profiling information would constitute personal data and be subject to the Data Protection Act. A user must be informed whenever a cookie or other tracking system enables the collection of personal data.

- Profiling visitors through IP addresses – Many Internet Protocol (IP) addresses, particularly those allocated to individuals, are dynamic. So each time a user connects to the Internet Service Provider (ISP), the user is allocated a different IP address. This means that only the ISP can link an IP address to an individual, and the profiling built up is not personalised. It is only if the same IP address is used each time that it may be possible to link an IP address to a particular computer which may actually or by assumption be linked to an individual user and therefore to develop personalised profiling. If this were the case the profiles would constitute personal data subject to the Data Protection Act 1998.

- Web crawling and spiders – These are software programmes used to collect e-mail addresses or other personal data from the Internet. Website operators should exercise caution when harvesting personal data from sources other than from the individual party. Those who use spiders are likely to breach the Data Protection Act 1998 unless they use the information for the purpose for which it was first made available.

- Web-bugs – These are graphics files designed to monitor who is reading a web page or e-mail message. Data controllers who intend to place a web-bug or similar device, should give the individual a simple means of refusing or disabling the device prior to any personal information being collected through it.

TRAFFIC DATA

Traffic data relates to the usage and billing profile of an electronic communications network's subscribers and users. No matter how a service provider wishes to process its traffic data, this data must be erased or made anonymous when it is no longer needed to transmit communications. In terms of e-mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

Traffic data may be processed for various specified purposes by persons acting under the authority of providers of the public communications networks and publicly available electronic communications services, but only to the extent and for the time period necessary. Firstly, traffic data may be processed to facilitate subscriber billing and interconnection payments. No consent of the subscriber is required for such processing, but the service provider must inform the subscriber of the types of traffic data to be processed, and the nature and duration of such processing.

Secondly, traffic data may be processed for the marketing of the electronic communications services or the provision of value added services, provided the subscriber has consented. Value added services may consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information. The subscriber's consent must be given on the basis of accurate and full information regarding the types of data the service provider wishes to process, the purposes and duration for which this would be done, the subscriber's right not to give his consent and his right to withdraw his consent at any time.

Thirdly, the service provider may process traffic data relating to subscribers where necessary in individual cases to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider to detect and stop fraud consisting of unpaid use of the electronic communications service.

LOCATION DATA

In digital mobile networks, triangulation-based technology may be able to generate information about the location of individuals from the transmissions of their mobile phone or other communication device. Location data may only be processed to the extent and for the duration necessary to provide a value added service, such as providing individualised traffic information or guidance to drivers. In any event, the location data must either be made anonymous or the subscriber must have consented to the processing. Such consent must be given on the basis of type of location data which will be processed, the purposes and duration of the processing, whether the data will be transmitted to a third party for the purpose of providing the value added service, the subscriber's right not to give his consent and his right to withdraw his consent at any time.

Processing may only be carried out by persons acting under the authority of the service provider or publicly available electronic communications services or of the third party providing the value added service.

APPENDIX

REGULATION OF UNSOLICITED COMMERCIAL COMMUNICATIONS

	E-Commerce Directive 2000/31	**Distance Selling Directive 97/7**	**Distance Marketing of Financial Services Directive 2002/65**	**Privacy & Electronic Communications Directive 2002/58**
Recipients to be protected	Natural and legal persons	Consumers i.e. natural persons acting outside their trade, business or profession	Consumers i.e. natural persons acting outside their trade, business or profession	Subscribers who are natural persons
E-mail to an individual	Suppliers must label unsolicited marketing e-mails as such Suppliers must consult and respect opt-out registers	Not permitted if the consumer objects	Member States to select either opt-in or opt-out	Consent required (but, permitted in respect of direct marketing of similar products or services to existing customers unless they object)
E-mail to a company	Suppliers must label unsolicited marketing e-mails as such	N/A	N/A	The legitimate interests of these subscribers should be sufficiently protected.
SMS message to an individual	N/A	Not permitted if the consumer objects	Member States to select either opt-in or opt-out	Consent required (but, permitted in respect of direct marketing of similar products or services to existing customers unless they object)
SMS message to a company	N/A	N/A	N/A	The legitimate interests of these subscribers should be sufficiently protected.
Telephone to an individual	N/A	Not permitted if the consumer objects	Member States to select either opt-in or opt-out	Member States to select either opt-in or opt-out
Telephone to a company	N/A	N/A	N/A	N/A
Automatic Calling Machine$^{\Phi}$ to an individual	N/A	Consent required	Consent required	Consent required
Automated Calling Machine$^{\Phi}$ to a company	N/A	N/A	N/A	N/A
Fax to an individual	N/A	Consent required	Consent required	Consent required
Fax to a company	N/A	N/A	N/A	N/A
Mail to an individual	N/A	Not permitted if the consumer objects	Member States to select either opt-in or opt-out	N/A
Mail to a company	N/A	N/A	N/A	N/A

NOTES

* N/A means that the Directive does not regulate unsolicited commercial communications to that category of persons using that type of medium.

$^{\Phi}$ An automatic calling machine makes calls without human intervention.

FURTHER RESTRICTIONS

- Data Protection Directive 1995/46 states that personal data must not be processed for direct marketing purposes (by means of any medium) if the individual objects.

CONTACT INFORMATION

If you would like to discuss any aspects of business or financial services regulation please contact:

John Casanova, Partner, Tel +44 (0) 20 7360 3739

Susan Atkinson, Associate, Tel +44 (0) 20 7778 1869

William Long, Associate, Tel +44 (0) 20 7778 1865

Sidley Austin Brown & Wood

1 Threadneedle Street

London EC2R 8AW

Tel: +44 (0) 20 7360 3600

Tel +44 (0) 20 7626 7937

WWW.SIDLEY.COM

ALL PARTNERS ARE EITHER SOLICITORS OR REGISTERED FOREIGN LAWYERS

REGULATED BY THE LAW SOCIETY