The Implementation of the E-Commerce Directive in English Law

By Clare Sellars,
Associate, McDermot, Will & Emery, London

email: csellars@europe.mwe.com

The Electronic Commerce (EC Directive) Regulations 2002/2013 [hmso.gov.uk] (the "**Regulations**") are the main UK legislation implementing the Electronic Commerce Directive (2000/31/EC) (the "**Directive**"). The Regulations largely came into force on 21 August 2002, except in respect of Regulation 16 which amended the Stop Now Orders (EC Directive) Regulations 2001/2555 and came into force on 23 October 2002.

The Regulations apply to EU and EEA countries and Gibraltar, but not the Isle of Man or the Channel Islands.

The Regulations should be reviewed together with various other relevant legislation e.g. the Electronic Commerce Directive (Financial Services and Markets) Regulations 2002/1775. The DTI has also published a revised Guide for Business which relates to the Regulations and additional guidance entitled "Complying with the E-commerce Regulations 2002". Although neither publication has any legal force, these publications assist to a large extent with the interpretation of the Regulations and should be reviewed accordingly. A brief summary of some of the main provisions of the Regulations is set out below, but this analysis should be regarded as an overview and not fully comprehensive.

The Regulations and the Directive – implementation issues in the UK

Generally, the prevailing view of the Directive in the UK was a positive one. The Directive was regarded as likely to encourage e-commerce and to result in a more coherent framework within which to provide information society services throughout the EU. The "country of origin" regulatory principle was generally supported.

There were, however, a number of contentious issues. For example, strong opposing opinions emerged in relation to the issue of unsolicited commercial communications. Most views favoured opt-out, but some views advocated a more severe approach. Disputes also arose as to how such communications should be identifiable.

One of the most significant contentious issues was the question of how to implement the Directive's provisions relating to limiting intermediary service providers' liability. Notably, diverse strongly held opinions developed relating to the issue of whether "notice and takedown" procedures should be introduced by statutory regulations, industry self regulation codes or both.

The Regulations differ from the Directive in a number of ways. For example, the Directive prohibits the imposition of general obligations on mere conduits, caches and hosts to monitor information they transmit or store. Neither may member states impose general obligations on such service providers to actively seek facts or circumstances indicating illegal activity. It was felt that no such obligations existed in English law at present and introducing them in the future would be incompatible with the Directive. The Regulations do not mention the issue of monitoring. However, the DTI's revised Guide For Business suggests that imposition of monitoring obligations in specific cases is not affected e.g. in compliance with a warrant issued under the Regulation of Investigatory Powers Act 2000 to secure the interception of a communication in the course of its transmission by means of a telecommunication system.

The DTI Guide also states that the Regulations also do not impose statutory obligations on service providers to promptly inform the competent public authorities of alleged illegal activities undertaken or information provided by their service recipients, or obligations to communicate to the competent authorities, on request, information enabling the identification of their service recipients with whom

they have storage arrangements. Existing statutory obligations continue to apply equally online as well as offline.

Another area where the Regulations do not reflect the Directive is in respect of Article 7(2) of the Directive, which requires service providers engaging in unsolicited commercial e-mail to consult regularly and respect the opt out registers where natural persons who do not wish to receive such communications can register. This is because it was felt that existing industry codes of conduct and self regulation effectively protect recipients of such communications. The UK has always adhered to the Direct Marketing Association's MPS register. The Communications Data Protection Directive (2002/58/EC) which must be implemented by Autumn 2003 will establish opt-in (or prior consent) requirements for unsolicited commercial e-mail sent to natural persons. An exemption applies where such e-mail is sent in the context of an existing customer relationship, as long as the relevant e-mail addresses are obtained according to the framework Data Protection Directive and addressees are always permitted to opt out of further communications. Businesses will be allowed to use electronic contact details obtained from customers during transactions for subsequent direct marketing of their own similar products or services, as long as customers obviously have the chance to object, easily and without cost, to such use when those details are collected and on the occasion of each message. Direct marketing e-mails will only be permitted in circumstances where subscribers have given prior consent and will never be allowed where the sender's identity is disguised or concealed.

Neither the Directive nor the Regulations proposed statutory "notice and takedown" procedures concerning the disabling or removal of access to information. The UK Government believed that industry codes of conduct and self regulation were sufficient in this area, but that even if they were not sectoral approaches would be suitable in the light of the different circumstances which would be relevant in each case. The Commission is, however, obliged pursuant to the Directive to report to the European Parliament every two years from 17 July 2003 in respect of a number of matters, including whether proposals relating to this issue and attributing liability following the taking down of content are necessary.

The Regulations' Content – an overview

What Do the Regulations Apply to?

The Regulations apply to the provision of "**information society services**", i.e. "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".

Which types of services do the Regulations cover? The Regulations are widely applicable, covering e.g. transmission and storage of electronic content, online business to business and business to consumer sales, provision of access to communications networks on-line, advertising over a variety of media and video on demand. Information society services are likely to include any services comprising an economic activity e.g. search, access and retrieval of data.

Services where the customer is physically present (i.e. not provided at a distance), services not provided "at the individual request of a recipient of a service" (which includes broadcast services generally) and using e-mail *per se* are excluded from the Regulations. Any services not provided by electronic means and communications between service providers and recipients via interactive digital television are also likely to be excluded.

What Do the Regulations Cover?

The "co-ordinated field" defined in the Regulations broadly sets out the requirements service providers must adhere to to provide information society services e.g. qualifications or authorisation, requirements regarding behaviour, quality or content of the service, or liability. Requirements relating to goods as such and the delivery of goods or services not provided electronically are not covered.

The Regulations also do not apply to a number of specified issues e.g. issues covered by certain data protection legislation, tax, "cartel law" and betting, gaming or lotteries.

The Country of Origin Approach

UK law requirements falling within the co-ordinated field apply to any information society services provided by a person from a UK establishment wherever the service recipient is located in the EEA, subject to certain derogations.

Unless the derogations apply, UK law does not apply to information society services provided by service providers established elsewhere in the EEA where applying it would restrict the freedom to provide that service into the UK. The Regulations provide that such "restrictions" would not include any requirement maintaining the level of protection for public health and consumer interests established by Community acts.

Derogations

Various derogations from the country of origin approach to regulation dis-apply the UK legal requirements in certain circumstances. The derogations include freedom to choose the applicable law of contracts, contractual obligations concerning consumer contracts, copyright and related rights.

Enforcement authorities may also take appropriate measures against given services on a case by case basis in certain cases, e.g. if necessary in the interests of public policy or consumer protection. Enforcement authorities must request the member state where the service provider is established to take appropriate measures before taking any action, except where the matter is urgent.

Information Requirements

Information society service providers are obliged to make certain information permanently, easily and directly accessible to recipients and relevant enforcement authorities in a form that is easily, directly and permanently accessible. Details of the main categories of information requirements are set out below:

General Requirements

Recipients must be provided with:

- full contact details;
- details of relevant trade organisations of which service providers are members;
- details of relevant authorisation schemes, including details of relevant supervisory authorities;
- professional details;
- VAT numbers (if applicable); and
- where relevant, clear price indications including tax and delivery.

Commercial Communications

Commercial communications (broadly electronic communications designed to promote (directly or indirectly) the service providers, goods, services or image) must be "clearly identifiable" as such and clearly identify the person on whose behalf they are sent. Promotional offers and related conditions must be easily accessible, clear and unambiguous.

Unsolicited Commercial Communications

Recipients must be able to identify on receipt both that these are commercial communications and unsolicited. This could probably be achieved by including the words "unsolicited advertisement" or "unsolicited commercial communication" in the e-mail subject line. These requirements relate to e-mail, but apparently not mobile text messages.

The Regulations do not require service providers to regularly consult and respect opt out registers. However, the Communications Data Protection Directive (2002/58/EC) will enforce a "soft" opt-in regime on direct marketers throughout the EU.

Electronic Contracting

In business to business transactions, unless otherwise agreed, where a contract is to be concluded electronically the service provider must provide certain information in a clear and unambiguous way before customers place orders. The information to be provided includes:

- the different technical steps necessary to conclude the contract;
- whether or not the service provider will file the concluded contract and whether it will be accessible;
- the technical means for identifying and correcting input errors prior to placing of the order; and
- the languages offered for the conclusion of the contract.

When concluding a contract, the Regulations provide that where service providers provide applicable terms and conditions to end users these must be made available so that they can be stored and reproduced.

Transactions

In business to business transactions, unless otherwise agreed, where end users place orders through technological means, service providers must:

- acknowledge order receipts without delay and by electronic means; and
- make available appropriate, effective and accessible technical means allowing end users to identify and correct input errors before placing orders.

The Regulations do not require order receipt to be acknowledged by the same electronic means that the order was placed by and this can probably be achieved by a confirmation appearing at the end of the ordering process.

The stage at which offers are made and by whom are not specified in the Regulations or the Directive. Electronic acknowledgement of customer offers could well constitute acceptance. In relation to contracts concluded exclusively by e-mail, the Regulations do not require acknowledgement without undue delay, making the point of acceptance even more uncertain.

Intermediary Service Providers

The Regulations limit the liability of intermediary service providers who provide services consisting of transmission or storage of information provided by the service recipient, or the provision of access to a communication network (although nothing prevents different contractual terms being agreed in respect of such limitation of liability). Notwithstanding this, any party may apply to a court for relief to prevent infringement of rights and administrative authorities retain power to prevent such infringement.

Mere Conduit

Service providers are not liable for damages, other pecuniary remedies or criminal penalties where the service providers are passive mere conduits of information for content providers, or simply provide access to communication networks, as long as the service provider did not:

- initiate the transmission;

- select the receiver of the transmission; and

- select or modify the information included in the transmission.

As long as service providers do not alter the integrity of information in transmissions, technical manipulations occurring during transmission will not constitute selecting or modifying the information and lead to liability.

Caching

If various conditions are met, service providers will escape liability for transmissions on communication networks consisting simply of "caching", i.e. the information is subject to automatic, immediate and temporary storage solely to make more efficient onward transmission of information to other service recipients at their request. The conditions are that the service provider must:

- not modify the information; comply with conditions on access to the information;

- comply with rules regarding updating of the information specified in a way widely recognised and used in the industry;

- not interfere with the lawful use of technology, widely recognised and used by industry to obtain data on the use of the information; and

- must act expeditiously to remove or disable access to the information upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, access to it has been disabled, or a court or administrative authority has ordered such removal or disablement.

Hosting

Liability is limited in relation to mere storage or "hosting" of information. If the service comprises merely storing information provided by a service recipient, the service provider is not liable for anything resulting from that storage as long as:

- he did not have actual knowledge of unlawful activity or information and, if a damages claim is made, was not aware of facts or circumstances from which it would have been apparent to him that the activity or information was unlawful;

- or on obtaining such knowledge or awareness he acted expeditiously to remove or disable access to the information.

This limitation of liability is not effective if the service recipient was acting under the authority or control of the service provider.

In deciding whether a service provider has actual knowledge in relation to the caching and hosting limitations of liability, a court must consider all matters which appear to be relevant in each case and among other things must consider:

- whether a service provider has received an appropriate notice; and

- the extent to which such notice includes the sender's full name and address and identifies the location of the information and the unlawful nature of the activity or information.

C.S.