SIDLEY AUSTIN BROWN & WOOD

London

EU REGULATION OF E-COMMERCE UNDER THE E-COMMERCE DIRECTIVE

The EU Commission has stated it believes that between 2001 and 2003, the number of people engaged in business online will have trebled and the number of transactions to buy and sell goods and/or services over the Internet will have multiplied by twenty. The UK's Department of Trade and Industry estimates that the e-commerce industry is worth in excess of £57 billion in the UK alone. One of the difficulties experienced by businesses that wish to conduct e-commerce is the increasing need to know not just about the legal requirements of their own jurisdiction, but also the legal requirements of those jurisdictions where their customers are located. Whilst for consumers one of the biggest hurdles is the continued lack of trust and confidence in the Internet as a means of purchasing goods and services.

In order to assist suppliers and customers to engage in e-commerce, the EU adopted the EU Directive on Electronic Commerce on 8 June 2000 (the "Directive"), which was required to be implemented into Member State law by 16 January 2002. The majority of Member States have not met this deadline no doubt partly due to the uncertainties that exist in implementation of the E-Commerce Directive into their national Member State law. In the UK the E-Commerce Directive was implemented by the Electronic Commerce (EC Directive) Regulations 2002, in force 21 August 2002. This briefing paper sets out how the E-Commerce Directive tries to tackle some of the principal issues facing e-commerce.

A Single European Market in Information Services

The aim of the Directive is to provide a single market in "information society services" throughout the EU. The Directive covers:

- requirements regarding the role of national authorities;
- transparency requirements for web advertising;
- principles relating to contracting online;
- limitations on the liability of Internet intermediaries; and
- requirements regarding disclosure of any codes of conduct, such as for online dispute settlement, by which the service provider is bound.

Information society services are defined as services normally provided for remuneration, at a distance, by electronic means and at the individual request of the recipient of the service.

To further the aim of a single market in information society services, the Directive provides that such services can be provided throughout the EU if the service provider complies with the law in its home Member State (i.e. the state in which it is established). This is known as the 'country of origin' principle. Under the Directive, information services providers ("ISPs") are "established" where they effectively pursue an economic activity using a fixed establishment for an indeterminate duration. Using this definition the following do not amount to establishment:

- the location of the technology used e.g. location of the server;
- the ability to access an Internet site in a Member State;
- the fact that the ISP targets services at the territory of another Member State.

Thus, in theory, ISPs in providing information services across the EU will only need to comply with one set of laws instead of the laws of 15 different Member States. However, there are a number of exceptions from the country of origin principle such as for:

- contractual obligations concerning consumer contracts;
- unsolicited commercial communications by email;
- advertising of units by collective investment schemes under the UCITS Directive;

In addition, host Member States may take measures to restrict freedom to provide information services if the measures are necessary for public policy, health, security or consumer protection. The result of these derogations is that businesses will need to consider carefully whether their activities will still be subject to the host Member State laws where their online services are received. It is even possible for different aspects of the same transaction to fall both within and outside the Directive.

For online financial service providers the effect of the Directive in determining which Member States regulations apply needs to be carefully considered.

Transparency of Information Service Providers

In order to encourage trust and confidence in consumers purchasing online the Directive requires Member States to ensure their national laws oblige ISPs to make information concerning their activities available to the recipients of the service in an easily accessible form. This information includes the ISP's name, geographic and email address, trade/company number, authorisation by any public or professional bodies and VAT number.

In addition, where ISPs refer to prices the Directive requires that these must be indicated clearly and unambiguously and indicate whether they are inclusive of tax and delivery costs. The aim is again to enhance the transparency of e-commerce.

Commercial Communications

The Directive also requires that commercial communications, which are defined widely to include any form of communication designed to promote goods or services and so would include electronic advertising and direct marketing, are clearly identifiable as such and the person advertising is identified.

The Directive provides that those Member States that permit unsolicited commercial communications by email must ensure that ISPs identify their unsolicited emails as such as soon as received by the recipient. ISPs must also consult and respect opt-out registers, that is registers on which consumers and businesses may register their wish not to receive unsolicited communications. However, under the proposed Communications Data Protection Directive unsolicited emails for the purposes of direct marketing will only be permitted to the extent consumers have given their consent[1].

Contracts Concluded by Electronic Means

The importance of knowing when online contracts are concluded has been graphically demonstrated recently in a number of cases where suppliers have advertised goods for sale on their web sites at incorrect prices and the suppliers were held bound to honour the online contracts with purchasers who accepted the offer before the supplier realised its mistake. For example, Argos mistakenly advertised televisions on its website for £3 each instead of £300. The Directive deals with certain aspects of concluding online contracts and provides that Member States are required to remove any prohibitions or restrictions on the use of electronic contracts, with certain permitted exceptions[2].

Member States must also ensure that the ISP provides certain information about the contract formation process before the placing of the customer's order, in particular to make clear:

- what steps the consumer must take and how the full terms and conditions of the contract can be accessed;
- how the customer can spot and correct errors; and
- the languages offered for the conclusion of the contract.

In terms of concluding online contracts the Directive does not provide exactly when an online contract is concluded but does provide that except where otherwise agreed by parties who are not consumers that where the recipient of the service places his order through technological means then:

- the ISP must acknowledge the receipt of the recipient's order without undue delay and by electronic means;
- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

Where contracts are concluded exclusively by an exchange of emails then the requirement for the ISP to acknowledge receipt of the recipient's order and the requirement to enable a consumer to correct inputted errors do not apply.

[1] For further details see Sidley Austin Brown & Woods London's briefing paper on the New EU Legal Requirements in Online Marketing.

[2] The four exceptions are (i) contracts that create or transfer rights in real estate; (ii) contracts requiring by law the involvement of courts or public authorities; (iii) contracts of suretyship; and (iv) contracts governed by family law.

The provisions of the Directive mean that suppliers will need to specify to consumers when and how the contract is formed by including in website terms and conditions details of how offer and acceptance are to occur.

Liability of ISPs

The Directive considers the liability of ISPs as intermediaries by categorising them according to what they do with the information rather than considering the specific nature of the information. Prior to the E-Commerce Directive a number of Member States were taking different approaches to the liability of intermediaries for third party information. For example, the UK had considered the position, as regards defamatory statements, from the point of view of whether the intermediary could be deemed to have actual knowledge of the defamatory statements. The Directive adopts the approach taken in Germany with the Multimedia Act of 1997 which distinguishes liability between information providers, hosting service providers and access providers. In adopting the German approach the Directive distinguishes between 'acting as mere conduit', caching and hosting.

Acting as a Mere Conduit

Where the ISP plays a purely passive role in acting as a simple conduit, for the transmission of data or access to a communication network with only transient storage of information, then under the Directive Member States must provide that the ISP shall be excluded from liability, whether for primary liability or as an accomplice, provided the ISP does not (i) initiate the transmission; (ii) select the receiver of the transmission; or (iii) select or modify the information contained in the transmission.

Caching

Where the ISP temporarily stores the information, for reasons of better efficiency of transmission of information, such as storing popular web sites on their server to assist easy access, then the ISP shall be excluded under the Directive from liability provided that the ISP meets a number of requirements. In particular, the ISP must not modify the information and must act expeditiously to remove or to bar access to the information, upon obtaining actual knowledge that access to the information at the initial source of the transmission has been barred.

Hosting

This is likely to be the most relevant category for many ISPs. It involves the ISP actually storing or hosting information provided by a recipient of the service, such as, hosting a company's web site or bulletin board. Under the Directive an ISP who performs hosting activities, is excluded from liability for the information transmitted provided: -

- it does not have actual knowledge that the activity is illegal and, as regards claims for damages, is not aware of facts or circumstances from which illegal activity is apparent; or

- upon obtaining such knowledge or awareness acts expeditiously to remove or to disable access to the information.

The difficulties caused by this are that it is not clear from the Directive what constitutes "actual knowledge" or what constitutes valid and effective notice to alert an ISP to illegal material.

The Directive provides that no general obligation should be imposed by Member States on conduit ISPs to screen or actively monitor third party content (including filtering it for illegal content).

Codes of Conduct and Out of Court Dispute Settlement

The Directive specifically requires Member States to encourage the drawing up and publication of Codes of Conduct regarding E-Commerce and that legislation of the Member States does not hamper the use of ADR schemes in e-commerce disputes.

The UK Government, like other Member States, supports both provisions and is already supporting the promotion of a number of conduct schemes drawn up by bodies such as the Alliance for Electronic Business and the Consumers' Association on Trust UK, and is intending to strengthen the powers of the Office of Fair Trading to police such codes of conduct.

Next Steps

1. Consider your web sites to ensure that your business is complying with E-Commerce Directive requirements for information to be provided to consumers;

2. Consider to whom your web site is directed. If it is directed at consumers in other jurisdictions then consider whether your information services will fall under one of the Directive's derogations from the country of origin principle.

3. If you conclude contracts online consider whether your contract formation process will be in accordance with the requirements under the Directive.

4. If your business uses email to do marketing consider the provisions in the Directive concerning unsolicited commercial communications but bear in mind the proposed Communications Data Protection Directive which will require a recipient's consent to receive such emails.

5. If your business acts as an intermediary for instance hosting third party content examine internal procedures as a whole to establish under the Directive what (and where possible reduce) exposure to liability for such 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*
- *William Long, Associate, Tel +44 (0) 20 7778 1865*
- *Susan Atkinson, Associate, Tel +44 (0) 20 7778 1869*

Sidley Austin Brown & Wood
1 Threadneedle Street
London EC2R 8AW
Tel: +44 (0) 20 7360 3600
Fax: +44 (0) 20 7626 7937
www.sidley.com

ALL PARTNERS ARE EITHER SOLICITORS OR REGISTERED FOREIGN LAWYERS