

Markt/2006/09/E
Service Contract ETD/2006/IM/E2/69

**STUDY ON THE LIABILITY OF
INTERNET INTERMEDIARIES**

COUNTRY REPORT – United Kingdom

Executive summary

November 12th, 2007

By Prof. Dr. Gerald Spindler,
Department of Civil Law, Commercial and Economic Law, Comparative Law,
Multimedia- and Telecommunication Law
University of Göttingen

Part 1: Legislation

The E-Commerce Directive was incorporated in UK law by the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) (the “E-Commerce Regulations”). The 2002 Regulations apply to judge-made and to primary and secondary legislation passed or made before the 2002 Regulations were made (regulation 3(2) of the 2002 Regulations). In relation to primary or secondary legislation that postdates the 2002 Regulations, the requirements of the Directive need to be considered in each case and, if necessary, specific provision made to ensure compliance with the Directive. In June 2007 the UK government introduced the Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 to amend the Regulations for the Terrorism Act 2006.

British law does not contain any explicit regulation with regard to hyperlinks, search engines or content aggregators. Following the DTI consultation the UK government concluded that currently there is no necessity for specific regulations in this area; however, it will await the review of the E-Commerce Directive by the European Commission when it publishes its second review report on the E-Commerce Directive.

Part 2: National Case Law

Currently there is hardly any relevant case law dealing with the E-Commerce regulations, since most court decisions related to this area date back to before the ECD. In particular, the notion of “actual knowledge” has not yet been defined by British courts. In *Bunt v Tilley* a notice given to access providers did not satisfy the requirements of Regulation 22 since it did not include details of the location of the information or of the unlawful nature of the activity or information in question. The court found it would have been wholly impractical for the defendant to monitor its servers for defamatory content about the plaintiff in any event. In addition the court held that the E-Commerce Regulations would not preclude an injunction (Regulation 20 (b)), but only apply to financial and penal sanctions. However, the injunctive relief sought against access providers by the plaintiff in the case was wholly disproportionate to any conceivable legitimate advantage. The granting of an injunction would be pointless in respect of a defendant who had no way of ensuring compliance with its terms.

In the *Godfrey v Demon* case dating back to 1999 the court decided that the defendant host provider was liable for damages since he had not removed defamatory content at the request of the affected party. The court held that, whenever the provider transmitted or allowed to be transmitted a defamatory posting from the storage of his news server, he *published* that posting to any subscriber to their internet service provider. Thus every

time one of the defendants' customers accessed the newsgroup and saw the defamatory posting in question, it constituted a publication to that customer.

In the linking case *Elton John & Ors v Countess Joulebine* the provider of a hyperlink became liable for damages once she became aware that information published on the website was confidential. Concerning deep links, the court in *Shetland Times v Wills* granted an injunction prohibiting the defendant from deeplinking and bypassing the plaintiff's front page by way of using headlines/links.

As regards claims for information, courts allow a cause of action against host providers operating discussion forums to disclose the identity data of their users in case of defamations (*Totalise v Motley Fool*) according to the Norwich Pharmacal rule. This line of jurisdiction was once more approved in the *Grant v Google* case where the court accepted a claim for information against a search engine operator.

Part 3: Notice and Take-Down Procedures

There is no statutory notice and take-down procedure in place in the UK. The DTI recently announced that it is considering sponsoring "an independent study on the need for a legislatively-backed notice and takedown and putback regime in the UK".

With regard to criminal offences, there is a notice and take-down procedure for notices of public authorities to host providers for content which constitutes an offence under the Terrorism Act 2006. The provider must comply with the notice within 2 working days. Failure to comply is not itself an offence, but may lead to the provider being charged with an offence under the Act. Regulations 5 to 7 of Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 incorporate Art. 12 to 14 ECD and create specific exemptions from liability for offences under sections 1 and 2 of the Terrorism Act for intermediaries providing mere conduit, caching or hosting services.

A number of self-regulatory bodies require compliance with laws such as the E-Commerce Regulations in their codes of practice. The Internet Services Providers' Association, UK (ISPA) has issued a Code of practice which, however, does not contain a formal recommendation for notice and take-down procedures but rather a kind of ombudsman procedure concerning complaints about a member of ISPA. The Internet Watch Foundation (IWF) is an industry organised body in the UK which works with Intermediaries on, inter-alia, the restriction on access to child abuse images. The IWF is operating a hotline to enable the public to report instances of potentially illegal content and a notice and take-down service to alert hosting service providers of criminal content found on their servers.