17th BILETA Annual Conference

April 5th - 6th, 2002.
Free University, Amsterdam.

"Don't Shoot the Messenger?" The Evolution of Liability for third Party Provided Content in the UK

Gavin Sutter
Research Fellow
IT Law Unit
Centre for Commercial Law Studies
University of London

Email: g.p.sutter@qmul.ac.uk

Introduction: ISPs & Third Party Liability

"Give him tending, he brings great news." So says Lady Macbeth on receiving the news of her husband's victory in battle and imminent return home from a weary messenger, dispatched by Macbeth himself. Had the news been bad, the messenger would have been severely beaten, as was the custom at that time. This tradition has, of course, long since died out in practice: in general, we no longer hold intermediaries responsible for the content when they are simply passing on a message. With, however, the arrival of the internet, or more specifically the world wide web, as a mass media in the early 1990s, it became often impossible or at least very difficult to track down the person with whom offending content originated. Whether that content be obscene publications, copyright infringements, or defamations posted to online newsgroups, the issue began to arise as to whether an ISP should, in certain circumstances, be held liable to remove or to block offending material. Is this fair? Is the ISP a co-conspirator who should face responsibility - or a mere conduit who cannot be blamed for the content? This paper considers the evolution of UK law in response to the position of ISPs and liability for third party content over the past several years.

There are three major types of content at issue in relation to ISP liability for material provided by third parties. Firstly, there is obscene material contrary to criminal law, such as paedophilic images, or those featuring acts of bestiality. Copyright infringement is significant in this context where, for instance, an individual takes advantage of an ISP's hosting service in order to establish a website with the purpose of trading in MP3 files which infringe copyright in the original sound recordings. Thirdly there is the issue of defamation: an ISP potentially faces liability for publishing a defamatory statement posted by a third party to a bulletin board service hosted by the ISP.

Liability for Obscenity

In UK law there is a gap between what is an illegal obscenity, and what is merely offensive to even a sizeable proportion of the general public. Thus stylised photographs of bare breasted young women as featured daily in several tabloid newspapers (and now often their associated websites), and much else besides, are perfectly legal. In order to be found illegal on grounds of obscenity, pornographic material must be of an extremely strong nature, generally featuring depictions of illegal behaviour, such as a young woman involved in an act of sexual congress with a dog. In *R -v- Anderson & Others*[1], the court found the legal definition of `obscenity' to be narrower than its "normal dictionary meaning" of "repulsive, filthy, loathsome...greedy, indecent, lewd". Under the regime set out by the Obscene Publications Acts of 1959 & 1964, material is "obscene" if it has a tendency "to deprave or corrupt" those likely to be exposed to it.[2] This is not limited to material of a sexual nature; in the late 1960s, Lords Parker CJ, Widgery and O'Connor JJ sitting in the Queens Bench Division, found the manufacturer of bubblegum cards intended for children, which featured explicit scenes of death and bloodshed in military warfare, to be guilty of having made obscene publications. The cards featured no depictions of acts of a sexual nature: the obscenity lay in the fact that the violent depictions were sufficient for the court to consider that they might "tend to deprave or corrupt" children who saw them.[3]

With the exception of paedophilic material[4], mere possession of an obscene article is not an offence under UK law. Possession with the intention of publication for gain, however, is an offence[5]; essentially this is the offence of making an obscene publication. This offence may be committed simply by making obscene material available for electronic transfer or downloading by another party who is thus enabled to access and copy that material.[6] It thus follows that an ISP which provides online access and hosting, in exchange for a subscription fee could face liability for an obscene website, created by a subscriber, hosted by the ISP and to which the ISP provides access. The transmission of obscene material via the internet can also amount to an offence under the Broadcasting Act 1990. This Act extended the Obscene Publications legislation to incorporate live and pre-recorded "programme services". The definition given "programme services" in the Act[7] is sufficiently broad to incorporate information transmitted over the internet.[8] Schedule 15 Paragraph 3 of the 1990 Act provides that an obscene article in the possession, ownership or control of a person who intends to include the matter recorded on it in a relevant programme is to be regarded as an obscene article had by that person for publication for gain. There are defences provided in the Act (along the lines of "did not know and had no reason to know"), however, while this remains untested before the courts, it is at least possible that an ISP could be held to be the publisher of an obscene article under this legislation.

So it may be said that where an ISP hosts a website containing obscene material provided by a third party and has the requisite knowledge, that ISP will face liability as the publisher of an obscene article. Such knowledge may be constructive (for example, in relation to a newsgroup with a title such as alt.pictures.youngteen.bondage), or involve actual notice of the obscenity. It has also been suggested that an ISP which provides internet access to a known publisher of obscene materials may face liability, even where the material in question is hosted on the other party's own server.[9] It would seem that ISPs are in a difficult position, however, in practice the UK has evolved a process for dealing with online obscenity, an alternative policy approach which avoids, as it were, shooting the messenger. There have, to date, been no prosecutions brought against ISPs with respect to obscene

material, and it is unlikely that such a case would arise in future unless an ISP was sufficiently aware and failed to act. The UK is fond of self-regulation where this works in place of law (see, for instance, the Advertising Standards Authority, or the Press Complaints Commission). In 1996, the Internet Watch Foundation was established, and a hotline set up to which members of the public can send notice of objectionable material that they have discovered online. In turn, the IWF will investigate complaints and pass on the details to the relevant ISP which will then delete the material and / or delete any reported links to it. The IWF, contactable via phone, fax, email and at www.iwf.org, has the backing of both government and industry, and has proven successful thus far.[10] Its focus is limited insofar as its stated main target is child pornography, however, it must also be recognised that this has been the main area of concern in recent years. The UK legal system can clearly be seen here as having evolved a new policy approach to deal with issues raised by the internet, not least ISPs. Now, an ISP which works with the system (and all ISPs are keen to be perceived as `good citizens', not least as this is much to their commercial advantage as much as it is ethical) to help remove obscene material can be surer that it will not, as a matter of policy, be made the target of an action in respect of the publication of obscene materials.

Copyright Infringement

Section 23 of the Copyright, Design and Patents Act 1988 sets out the offence of secondary copyright infringement. A person may be liable where he is both in possession of the infringing copy in the course of a business, and he knows *or has reason to believe* that the material he is holding constitutes an infringing copy of a copyright work. Dealing with the first element, an ISP will clearly fall within the definition of a business under the Act.[11] An ISP which hosts material is clearly in possession of it. Where the issue of possession is not so clear is in relation to situations where an ISP is merely acting as a pass-through provider, or even caching material: is such transitory copying sufficent to constitute possession? These issues are being addressed by the EU (see below), however in any case, in such instances even if there was possession, the requisite knowledge element is unlikely to be present.

Knowledge in this context can be difficult to pin down. Actual knowledge is a simple issue, however, the boundaries of constructive knowledge ("reason to believe") are somewhat blurred. In the online environment, there is a high likelihood that infringing copies will be present. For example, the alt.binaries.warez* newsgroup, where reportedly 90% of postings contain or are themselves infringements. The last several years have seen a boom in online trading of MP3 files which looks set to continue (despite the demise of Napster following the resignation of founder Shawn Fanning and CEO Konrad Hilbers on 14 May 2002) for some time to come. Far and away the majority of MP3 files being traded online are infringing copies. The question arises whether such constructive knowledge is sufficient for a finding of liability on the part of an ISP which hosts the material. The mere fact that there is a high likelihood of the presence of infringing copies does not automatically mean that an ISP has the requisite awareness to face liability under section 23. There is as of yet no case law in respect of this provision, however, two cases in particular decided under the equivalent provision in the previous Copyright Act of 1956 merit consideration. In *Hoover plc -v- George Hulme Ltd*[12] the court gave strong support to the theory that actual knowledge of an infringement is required. Five years later, in *Columbia Picture Industries -v- Robinson*[13], it was held that a general knowledge that some copies may be infringing did not constitute sufficient knowledge for secondary copyright infringement.

Amongst other provision designed to update and harmonise copyright law as it relates to the online environment, the EU has passed the Copyright in the Information Society Directive. This Directive grants a number of key rights to copyright holders. These include the "reproduction right"[14], the "right of communication to the public"[15], and the "distribution right."[16] Such exclusive rights may well put ISPs in an awkward position, however, the Directive also provides an exemption from the reproductive right where the ISP is merely acting as a pass through provider, transmitting the information.[17] It must also be remembered that the exemptions from liability provided in the Ecommerce Directive will work in conjunction with this Copyright Directive in order to ensure that ISPs are not unfairly exposed to heavy liability for third party provided content. It remains to be seen how the UK parliament will amend UK copyright law in order to comply with the Copyright Directive.

Defamation

The general rule of English defamation law is that the publisher of a defamation faces strict liability. However, the current legislation, the 1996 Defamation Act, was passed at a time when internet technology was rapidly entering the mainstream and the web, already a cultural phenomenon, was swiftly being colonised by commercial interests. The position of internet intermediaries was much debated, and, parliament accepted that an ISP should not be treated in the same manner as a traditional publisher.[18] Under the Act as passed, an ISP will have a valid defence where defamatory material is posted to its servers if it is not the "author, editor or publisher" of the defamation, *and* it did not know and had no reason to believe that the statement in question was defamatory, *and* the ISP took reasonable care in relation to the publication of the statement in question.[19] Is an ISP a publisher under the Act? Per Section 1(3), an ISP will be exempted from categorisation as a publisher where certain conditions are satisfied[20]; under the conditions as set out in the Act, ISPs are highly unlikely to be considered publishers.

It must be noted that while it provides them with a defence, Section 1(3) also gives rise to something of a dilemma for ISPs. There is a very fine path for ISPs to tread between the requirements in section 1(1) - that they did not know and had no reason to believe the material was defamatory and took reasonable care in relation to its publication, as well as the requirement to take steps to remove offending material on receipt of actual knowledge - and going too far in monitoring their servers, which may result in the ISP falling outside the exemption in section 1(3) and facing liability as a publisher.

The first UK case on ISP liability for defamation was *Godfrey -v- Demon Internet*[21], a preliminary hearing in order to establish whether the ISP could escape liability by virtue of section 1, the so-called defence of "innocent dissemination". The facts were that a third party posted a message to the soc.culture.thai newsgroup, which Demon hosted but did not actively monitor, stating, essentially, that all Thai women were intellectually deficient and as a result were only suited to employment as prostitutes. The message claimed to be from Mr Godfrey, but was apparently posted by another party. Godfrey contacted Demon and demanded that the posting be removed as it was defamatory of him, however, Demon failed to remove the posting before it expired automatically some two weeks later. Demon sought to rely upon the defence in Section 1, however, it was ruled not to be open to them. While the ISP was considered not to be a publisher for the purposes of Section 1 of the 1996 Act, it was found to be liable for the defamation from the point at which it received actual knowledge of the posting. Significantly, the court held that the defence

would be valid in respect of the period up to that point. In future cases, in the absence of actual knowledge, presumably when seeking to determine whether the ISP took reasonable care in relation to the publication and had no reason to believe that it was defamatory the courts would look to the nature of the newsgroup. Demon may similarly have been unable to take advantage of the defence in the absence of actual knowledge if the posting was to a newsgroup entitled, for instance, "Scandalous B'stards", and which had a reputation for and was designed to solicit postings of a potential defamatory nature.

Although decided very squarely within the specific context of the Defamation Act, the principle in *Godfrey* may well be applied elsewhere by analogy: an ISP which has been notified (and hence has actual knowledge) of the nature of certain third party provided content which it is hosting may face liability in respect of that content.[22] While it is, *prima facie*, a straightforward decision and Demon were clearly at fault for failure to remove when in receipt of actual knowledge, this case has been controversial amongst civil liberties interests in the UK. Such groups have argued that an ISP approached and told that a particular posting is defamatory will not take the risk of considering whether the posting is in fact defamatory, but will simply remove it without question, well aware that Demon ended up paying out around half a million UK pounds for its failure do so. Concerns centre upon situations which may arise where this is abused by parties with something to hide. For instance, where an individual sets up a website on the ISP's servers which contains an article about "the Big Tick" training shoe company and its exploitation of child labour in sweatshop conditions in the Third World. In this scenario, the article, which happen to be true and can be fully substantiated, would be rapidly removed by the ISP on receipt of notification from the company's corporate lawyers rather than risk a lawsuit. Clearly this would be the only sensible commercial decision on the part of the ISP, however, freedom of expression would appear to be left vulnerable in such a situation.

The question of ISP liability has now been addressed at European level. The Ecommerce directive contains several provisions which seek to limit ISP liability for third party content in general. There are four main articles at issue here, the first being Article 12, which is concerned with the situation in which the ISP is a "mere conduit" - a pass-through provider which merely passes on information provided by a third party customer, exercises no control over the content of transmissions, and does not store them any long than is strictly necessary to facilitate transmission: what the Directive refers to as "automatic, intermediate and transient" storage. This immunity is to be granted on the proviso that at national level an ISP may be required to terminate or prevent an infringement, however, this would be carried out as a result of a court order and thus the ISP would have actual and official notice. Clearly the Article is designed to prevent an ISP from being held liable for the transmission of a data stream, the content of which it could not be expected to be aware.

The Directive gives a clear outline of what qualifies as caching for the purposes of the Article 13 immunity. Content must be provided by a third party, and be subject only to "automatic, intermediate and temporary storage" which makes the transmission to another third party more efficient. This immunity is lost upon receipt of actual notice that particular content has been removed or disabled, or ordered to be so, on grounds that it is contrary to law. Again, a national court may order the ISP to cooperate in terminating or removing an infringement.

Article 14 is, arguably, likely to prove the most significant immunity in practice. This article

grants ISPs an exemption from liability in respect of content which they host on their servers but which has been provided by a third party. The ISP must have no awareness of the illegal nature of the material in question, either directly or indirectly through facts or circumstances which render the illegality apparent. Once in receipt of actual notice, an ISP must act promptly to remove the material thus identified. The importance of such a qualified immunity for ISPs is readily apparent: unlike a traditional publisher, an ISP cannot be expected to be aware of all material which subscribers may have uploaded to its servers. Knowledge of the illegality is especially important in relation to defamation. For instance, if an ISP is aware that a particular posting exists, then it should be able to make a reasoned judgement as to whether that posting is obscene. However, as is often the case with defamatory statements, even if the ISP was directly aware of a particular posting, it may not be in possession of certain other facts necessary to be notified of the defamation. In *Godfrey*, the only indication that the posting in question may have been made by someone other than the plaintiff was a misspelling of his name. It would seem that Article 14, once transformed into UK law, is likely to effectively apply *Godfrey* to ISP liability for all form of third party content (despite the fact that *Godfrey* was decided within the very specific context of Section 1 of the Defamation Act 1996).

Article 15 sets out a general principle which relates to all the services covered by Articles 12, 13 and 14 (transmission, caching and hosting). Put simply, Article 15 requires that member states do not impose upon ISPs any general obligation to monitor information passing through or hosted on their systems. Again, however, this provision is qualified: national governments may still impose duties which require that some level of care be taken in relation to what is stored or transmitted. Member states may also impose a duty to promptly inform the appropriate authorities where notice is received of illegal activities or such are discovered. ISPs would also be expected to remove the information in a prompt manner. Further, the option is left open for member states to oblige the handover of identification details in respect of an ISP's subscribers with whom they have an agreement to provide host services.

In the UK, the DTI (Department of Trade & Industry) began public consultation on enactment of the directive during August 2001. Prior to the beginning of this consultation period, all indications were that, in line with general UK government policy on the internet, statutory regulation would be kept to a minimum and emphasis would be placed upon use of codes of conduct drawn up by industry bodies such as the Internet Service Providers Association, in line with Article 16 and Recitals 412 and 49 of the Directive.[23] This, as we have seen, is already an established approach in the UK in dealing with internet child pornography.[24]

Responses to the consultation, which closed in November 2001, by and large welcomed the Directive's provisions, however, a number of problem issues were identified. Many identified the need for codes of conduct to clarify certain technical issues in relation to transmission and caching. Regarding hosting, as the official summary of responses notes, "[t]he biggest single stumbling block was perceived to be the difficulty of imposing upon ISPs etc the task of deciding whether some content on their service is illegal or not." Further, two ISP respondents discussed their experience of receiving complaints about information hosted by them on a daily basis, many of which were false and often appeared malicious in intent. A large proportion of respondents to the consultation raised the issue of the `notice and take down' procedures which it would be necessary to implement in order to comply with the Article 14 requirements on notice. An industry code setting out the

procedure to be followed was a popular suggestion, although several also felt that such a code required statutory backing and even reserve powers permitting the government to impose a statutory scheme should this prove necessary. The lack of a standardised form of notice at present was considered to be a problem. Several respondents, particularly ISPs, argued that some form of `safe harbour' provision, whereby an ISP would not be liable either for wrongful takedown or wrongfully failing to take down material provided that they had followed the procedure in good faith, should be written into any industry code of practice.[25]

In early 2002, the DTI issued a second consultation on the Electronic Commerce Directive, this time accompanied by the draft Electronic Commerce (EC Directive) Regulations 2002. The draft Regulations, in the main, repeat the wording of the Directive almost verbatim. [26] Section 20 provides that nothing in the preceding sections relating to transmission, caching and hosting is to act in order to "prevent a person agreeing different contractual terms", and, further, nothing in the Regulations is to affect the rights of an aggrieved party to sue over an infringement of any rights. What is still lacking, however, is any effort to address the situations in which freedom of expression may be suppressed by ISPs who will not be prepared to run the risk of making a `wrong call' when they are in receipt of a lawyer's letter demanding that certain identified material be removed. It is still possible that a system for reposting of material which has been removed pursuant to notice of alleged illegality could be incorporated into an industry code of conduct on the application of the Regulations, however, it is regrettable that the government appears to intend to implement the regulations prior to such a code being at least made available in a draft form.

ISP Liability in the USA

Just as the USA adopted the internet as a mass communication tool some time earlier than the UK, so too the US has several years more experience in dealing with the legal issues raised by the need to regulate the online environment. A consideration of how the US legislature and courts have dealt with the problems now faced by the UK is therefore of interest.

ISPs & Copyright Infringement - USA

Early case law on ISP liability for third party copyright infringement shows that in the initial stages there was a great deal of confusion as to how to apply traditional copyright concepts online. In *Playboy -v- Frena*[27], the operator of a bulletin board service was held liable for uploading infringing material despite the fact that while it was the BBS operator's system which did the copying, it was enacted by a third party. In a similar situation in *Religious Technology Centre -v- Netcom*[28], the judge refused to hold an ISP guilty of copyright infringement on the ground that liability could only arise where there was a clear intent to copy. This intent was deemed not to be present where the action of a third party caused the copy to be made. Yet in *Playboy -v- Webbworld*[29], the fact that no control over the use by third parties of Webbworld's system to make infringing copies was possible was held not to be an issue: the company, the court held, should not be operating a business if that business could not be made to operate within the law.

In 1998 the Digital Millennium Copyright Act was enacted, ratifying the WIPO Copyright Treaty and updating the copyright regime to cope with internet technology. Within the specific context of intermediary liability for third party copyright infringement, the DMCA

makes similar provisions to those granted in general by the Ecommerce Directive.[30] Immunity from copyright infringement is granted to pass-through providers whose systems automatically transmit material provided by a third party. The material must be transmitted without being tampered with by the service provider, and only as an automatic response to commands from a third party. Recipients must not be selected by the service provider, and material may only be stored in the system for as long as it is required to facilitate the transmission. Broadly the same provisions are made in relation to caching, with the addition of duties to comply with conditions which may be imposed by the content provider, such as limitation of access to only those who have paid an associated fee, as well as to promptly remove copyright infringing material upon actual notice of same. A qualified immunity from liability for hosting copyright infringements where the material is provided and uploaded to the ISP's servers by a third party. This immunity is conditional upon the fact that the ISP has neither actual knowledge of the infringement nor any awareness of "facts or circumstances" from which the infringement is apparent. When in receipt of notice, an ISP must ensure that the material complained of is promptly removed from its servers. Further, an ISP which retains the right and ability in its system to control the activities of subscribers in relation to the material that the ISP hosts will not be able to benefit from the immunity where it has directly benefited financially from the infringement. Any infringement must be removed or blocked once notice has been received.

As well as its similarities to the provisions in the Ecommerce Directive, there is one particularly notable difference: provisions relating to reposting of material removed pursuant to a complaint.[31] Under the DMCA, an ISP will not face any liability towards any aggrieved party where it has acted in good faith to removed claimed infringing material. The exception to this rule lies in respect of material which, at the direction of the subscriber, is being hosted on the ISP's servers and is removed pursuant to a notice claiming copyright infringement. In order to be able to take advantage of immunity in such a case, the ISP must take reasonable steps to ensure that the subscriber is promptly notified that the material has been removed and/or comply fully with the reposting provisions. Effectively these offer the subscriber a right of appeal, the opportunity to be able to have their legitimate rights upheld where material has been unfairly removed. The inclusion of such a reposting procedure in the final version of the Ecommerce Regulations would do much to address the feared threat to free speech discussed above.

ISPs & Civil Liability USA

Outside the field of copyright, there is a general and very wide immunity from civil liability for third party content available to ISPs under US law. This immunity lies in the Communications decency Act of 1996. The CDA was much vilified at the time of its passage due to other provisions which created new offences in relation to online pornography and its availability to minors, and which were eventually found unconstitutional and struck out by the Supreme Court in the landmark *ACLU -v- Reno*[32] decision. Section 230, however, remained in force. This, so far as is here material, states:

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"

"[It is the policy of] the US to preserve the vibrant and competitive free market that presently exists for the internet and other interactive computer services, *unfettered by federal or state regulation*... Congress made a policy choice...not to deter harmful online

speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages... the specter [sic] of tort liability in an area of such prolific speech would have an obvious chilling effect. Congress...chose to immunize [sic] service providers to avoid any restrictive effect."

The leading case in interpreting this remaining fragment of the original Act is *Zeran -v- America Online*[33]. In this case, AOL were found not to be liable for a defamation posted to their servers by a third party, despite the fact that they had received *actual* notice of the defamatory post and had failed to act. The facts were, in essence, directly comparable to *Godfrey*; the decision, however, was extremely different. The judgement in *Zeran* made reference to the fact that a key intention of the immunity was to encourage ISPs to adopt a `good Samaritan' role in relation to content monitoring, without fear of becoming liable for content that should be removed but which goes unnoticed by them. *Zeran* confirmed that Section 230 overrules the *Stratton Oakmount -v- Prodigy*[34] case. In this case, the defendant ISP was found liable for third party content as a result of having held itself out to be a "family friendly" service, having taken active steps to monitor content, thus assuming a level of editorial control and with it responsibility for the material. Whether ISPs will in ptractice take it upon themselves to be the moral guardians of society in the way envisaged by the CDA's drafters is quite another matter. Other case following *Zeran* have confirmed the wide extent of the exemption from liability provided by this remaining fragment of the CDA.[35]

Concluding Remarks

UK strategy for dealing with ISPS in respect of third party provided content is set to continue to evolve for some time to come. A policy of requiring the intermediary to remove material which is contrary to law is often the best available option in the online world where it is often very difficult or even impossible to track the source. However, while the UK may have adopted this approach to controlling online content, increasingly the law is reflecting a wider global trend towards a "don't shoot the messenger" approach to ISP liability in this context. The reliance upon extra-legal systems such as codes of conduct for industry self regulation in place of extensive legislation is a long-standing approach which the UK has taken in a number of areas such as advertising (Advertising Standard Authority) and ensuring that certain ethical standards are observed by the press (Press complaints Commission). Already the UK has begun to take this approach in relation to internet content: rather than compel ISPs to assist in the tracking down of child pornography, both UK governments since 1996 have given their full support to the Internet Watch foundation, an industry based (and backed) body working in conjunction with the police to ensure that where paedophilic material is detected it is quickly removed from circulation and any details which may help to identify the perpetrators are promptly pass to the appropriate investigating authorities. Much as UK based ISPs may wish it were otherwise, the UK is unlikely to ever be as liberal in its approach as the US has been in recent years in relation to general civil liability - UK exemptions from liability, in common with the rest of the EU, are likely to remain qualified.[36] In any case it must also be remembered that the situation in the US post *Zeran* came about by accident rather than by the design of the original Communications Decency Act.

It remains to be seen how effective in practice the qualified immunities provided in the Ecommerce Directive and the plans for implementation of the same in the UK will be. There remains a lack of clarity in relation to certain concepts, such as what qualifies as "notice",

the boundaries of constructive knowledge, and so on. Larger companies with experienced legal departments may not find this presents too great an obstacle, however, it may be insurmountable for individuals with no legal background, such as an independent trader in second hand cars who discovers that the photographs which he has taken of his stock and placed online (his copyright works) have been infringed by another party. There is a strong need for guidelines to be provided so that such an individual has the same access to the legal process in order to protect his rights as a large company. The codes of conduct which the government plans to rely upon in order to provide much needed guidelines to the practical implementation of the Directive should address such issues, however, it is to be lamented that not even a draft version of such codes has been made available during either stage of consultation in order that especially the Draft Regulations may be read in their proper context, not on trust that certain areas will be clarified at some future date.

As to the question of the perceived threat to freedom of expression - ISPs removing legitimate material, such as a site recording human rights abuses by a multinational company, in order to evade liability where the complaint has been unscrupulous and the information true - it remains to be seen whether this will indeed be a problem in practice. Inclusion into the Regulations of some form of reposting provisions, along the same lines as those provided in the USA in respect of copyright infringement claims, would be a sensible move, providing a right of appeal and enabling the ISP to make a reasoned decision as to whether a complaint is vexatious or valid without fear of being penalised for acting in good faith.

We can chart the evolutionary development of a UK policy on ISP liability for third party content and speculate as to the likely future consequences, but in the last instance we can but wait and see whether such postulations prove to be the case.

---

[1] [1971] 3 All ER 1152

[2] Obscene Publications Act 1959 Section 1(1)

[3]*DPP -v- A. and B.C. Chewing Gum Ltd.* [1968] 1 QB 159

[4] See Protection of Children Act 1978 Section 1, as amended by the Criminal Justice and Public Order Act 1994

[5] Obscene Publications Act 1964 Section 1(2)

[6]*R -v- Fellows & Arnold* (1996) *The Times* 27 September

[7] Per Section 201 of the Broadcasting Act 1990, a "programme service" includes:

"...any other service which consists in the sending, by means of a telecommunications system, of sounds or visual images or both...for reception at two or more palces in the United Kingdom (whether they are so sent for simultaneous reception or at different times in response to requests made by different users of the service)."

[8] It may also be added that the Court in *Shetland Times Ltd -v- Wills* ((1997) *The Times*

21 January) remarked obiter that a web page may be considered to constitute a cable programme service.

[9] Smith GJH (Ed) [1997] *Internet Law and Regulation* 2nd Edition, FT Law & Tax, London, p.259

[10] According to its own annual reports, available on the website, and which the author has not yet found any reason to distrust.

[11] See Section 178

[12] [1982] FSR 565

[13] [1987] ChD 38

[14] Article 2: "...the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part..."

[15] Article 3: "...the exclusive right to authorise or prohibit any communication to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them..."

[16] Article 4: "...the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise..."

[17] See Article5

[18] which has much more control over material it publishes as compared to a hosting ISP where the publication process is rapid, automated, and content of a particular website, which can be one of thousands, may change overnight.

[19] Defamation Act 996 Section 1

[20] Section 1(3), so far as is here relevant, states:

"A person shall not be considered the author, editor or publisher of a statement if he is only involved-

...

(c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;

...

e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.

[21] *The Times* 20 April 1999

[22] Indeed it may be noted that while *Godfrey* was not actually cited, when Demon / Thus plc later appealed for an ISP-specific exemption to strict liability regarding the breach of a general media injunction against the publication of any information likely to lead to the whereabouts of Thompson and Venables, the infamous `Bulger murderers', the injunction was amended by Dame Elizabeth Butler Sloss, President of the family Division, to provide a similar defence.

[23] "The Government's approach is to legislate on internet and ecommerce related issues only as a last resort, and depend to the extent possible on leadership and self-regulation by those most directly concerned." (taken from Author's correspondence with DTI)

[24] See discussion of the Internet Watch Foundation, above; also www.iwf.org.uk

[25] See *DTI Consultation on Implementation of the Directive on Electronic Commerce (2000/31/EC) Summary of Responses*, available at www.dti.gov.uk
[26] See sections 17, 18 &19, c/f to Articles 12, 13 & 14 of the Directive

[27] 839 F Supp 1552 (MD Fla, 1993)

[28] 907 F Supp 1361 (ND, Cal, 1995)

[29] 968 F Supp 1167 (ND Ill 1997)

[30] See US Copyright Act Section 512, as inserted by the Digital Millennium Copyright Act

[31] See US Copyright Act Section 512(g), as inserted by the Digital Millennium Copyright Act

[32] 929 F Supp 824 (ED Pa 1996)

[33] 129 F 3d 327 (4th Cir. 1997)

[34] 23 Med. LR 1794 (SC Nassau County 1995)

[35] See, for instance, *Blumenthal -v- Drudge* 992 F Supp 44, 51-52 in which an ISP was held not to be liable for defamatory statements made by a gossip columnist and stored n their servers, despite the fact that the ISP exercised editorial control over the columnist. In *Ben Ezra, Wenstein & Co -v- America Online* (D.N.M. 1999), erroneous stock values attributed to the plaintiff company were held not to give rise to liability on behalf of the ISP as the information had been provided by a third party.

[36] The author would consider that this is a positive factor: unfettered liberalism is not always an unqualified good.