

10 June 2003

**Please note:** this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

## Table of Contents

1 Introduction .....	1
2 FE/HE Institutions as Internet Service Providers .....	1
3 Definition of an ISP .....	2
4 Liability for Obscene Publications .....	2
5 Liability for Defamation .....	4
6 Liability for Third-party Copyright Infringement .....	7
7 What is to be Done? .....	11

## 1 Introduction

The potential liability of internet service providers (ISPs) in relation to content provided by a third party has provoked much debate in the UK since 1999, when the Godfrey -v- Demon judgement became the first UK case to find such responsibility on the part of an ISP.

The state of ISP liability law in the UK has implications not only for commercial enterprises, but also for educational establishments providing internet access and information storage facilities for staff and students.

It has happened in the past that individuals have used such network access to download and store paedophilic images, or material which is otherwise obscene. Many are less than careful as regards the accuracy of information they pass on - one person's harmless email gossip is another's defamation. It is also increasingly common to find that many are taking advantage of high-speed access and free storage to facilitate peer-to-peer downloads of copyright infringing material.

This paper will consider the extent to which FE/HE institutions may face liability in respect of information which is accessed via, or stored on their networks. Several pertinent provisions of UK law will be considered, including, in particular, the Electronic Commerce (EC Directive) Regulations 2002, which give effect to, inter alia, the Electronic Commerce Directive's provisions with respect to ISP liability in this area.

Circumstances in which liability may arise will be identified, be that liability for making obscene publications, publishing a defamation, or copyright infringement. The paper will then advise on best practice for an institutional response in such circumstances, as well as measures which may be adopted as part of a risk-limitation strategy.

## 2 FE/HE Institutions as Internet Service Providers

One question which often arises in this context is: who is the ISP? Is each individual FE/HE institution at some level an ISP?

There is a persistent view that only UKERNA, as operators of the JANET network, would incur liability as an ISP. In actuality, it is the case that each individual institution faces potential liability in respect of information provided by third parties.

As this article will explain, ISP liability, as it has evolved in UK law, is in part founded in possession and control of content, for instance, the presence of copyright infringing or obscene material on an institution's servers.

### **3 Definition of an ISP**

Since July 2002, we must also consider the requirements of the Electronic Commerce (EC Directive) Regulations 2002, which give effect to the European Electronic Commerce Directive.

The "service provider" referred to in the part of the Regulations dealing with intermediary liability is defined as "any person providing an information society service" (Regulation 2(1)).

For the purpose of these Regulations, an "information society service" is given the same definition as that in Article 1(2) of European Directive 98/34/EC (the Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/EC of 20 July 1998);

That Directive defines 'service' as follows:

'any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'

For the purposes of this definition:

'at a distance': means that the service is provided without the parties being simultaneously present,

'by electronic means': means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,

'at the individual request of a recipient of services': means that the service is provided through the transmission of data on individual request.

Commercial ISPs are clearly covered by the terms of the Directive.

As regards FE/HE institutions, the key part of this definition is the phrase "normally provided for remuneration."

FE/HE institutions' internet services may not operate along the commercial model which involves direct remuneration, however, although the definition suggests that the commercial ISP is the norm, it certainly does not exclude those who offer such services without seeking remuneration.

The other elements of the definition clearly apply to the internet linked network services which educational institutions typically provide, and thus the individual institution is both obliged to meet the requirements and enjoy the limitations upon potential liability set out in the Electronic Commerce (EC Directive) Regulations 2002.

## **4 Liability for Obscene Publications**

### **4.1. Introduction**

Since the advent of the world wide web as a standard campus service for students, FE/HE institutions have been concerned about the accessibility of pornography online.

Pornography, of course, is not illegal in the UK. The usual motivation for a ban on its access via campus network terminals is concerned with preventing it being used in a manner which might constitute sexual harassment. Even the old question of management of limited resources may be relevant, as institutional funds provide the hardware and internet access for educational purposes, not so that students (or staff) can use them to view pornographic material.

There is, however, much material available on the internet which crosses the divide between the merely pornographic and the obscene.

Institutions must be concerned not only to prevent their networks being used to store or access such material, but also to ensure that they are not found liable for making an obscene publication.

#### **4.2. Definition of Obscene**

The courts have held that the legal definition of "obscene" is much narrower than its common, dictionary meaning (see, for example, *R v Anderson & Others* [1971] 3 All ER 1152).

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 (Obscene Publications Act 1959 Section 1(1)). 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, to be guilty of having made obscene publications. The cards featured explicit scenes of death and bloodshed in military warfare, but 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 (*DPP -v- A. and B.C. Chewing Gum Ltd.* [1968] 1 QB 159).

#### **4.3. Present Law as it applies to FE/HE**

With the exception of paedophilic material, mere possession of an obscene article is not an offence under UK law. However, possession with the intention of publication for gain is an offence (Obscene Publications Act 1964 Section 1(2)). 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 (*R -v- Fellows & Arnold* (1996) *The Times* 27 September).

In other words, an ISP that provides online access and hosting facilities 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.

It is conceivable, if not very likely, that a student or member of staff who benefits from the provision of institutional internet facilities might abuse them by creating a pornographic website which is sufficiently extreme as to be considered obscene by law.

While potential ISP liability under the Obscene Publications legislation remains a matter of conjecture, it is unlikely that a FE/HE institution could be liable in this respect.

The crucial issue here is in relation to the concept of "publication for gain".

Where no subscription fees are received by the institution, it is at best highly tenuous to argue that any funding which might come from an individual student's fees, feeds directly into the budget for maintaining the computer network (which is not a profit making activity). Staff, of course, do not contribute to the institution on a personal monetary level.

Of course, should an institution uncover material on its network which it considers may be obscene, and thus a matter for more than just internal disciplinary action, this should be reported to the police with all due haste.

#### **4.4. Child Pornography**

An area of major concern online, and one which has often dominated media coverage of internet crime during recent years, is child pornography. Unlike other obscene material, the mere possession of child pornography is an offence in the UK law. The creation (or facilitating the creation) of an indecent image of a child is an offence under the Protection of Children Act 1978. Section 160 of the Criminal Justice Act 1988 goes further and provides that:

"It is an offence for a person to have any indecent photograph or pseudo-photograph of a child in his possession."

A "pseudo-photograph" is a new concept, introduced by the Criminal Justice and Public Order Act 1994 as a response to advancements in home computer technology. Images which appear to involve children can be produced simply and rapidly using an off-the-shelf software package as simple as MS Paintbrush, or Photoshop. For example, body-parts such as breasts can be resized and other adult sexual characteristics such as body hair removed. In such images it is also common for a child's head to be superimposed on top of the altered body image. The 1994 Act also broadened the definition of "photograph" to include images in electronic data formats.

Pseudo-photographs are treated by UK law as being in every way equivalent to a pornographic image featuring a 'real' child.

The paedophiles who create these images often store them in hidden files on ISP network servers. It is a very real possibility that a FE/HE institution's servers might be used to store such material.

For example, in *R v Fellows & Arnold*, (cited above) the defendants, who were found guilty of various offences in relation to child pornography, were employees of the University of Birmingham, and were actively seeking to create a large, internet-accessible database of paedophilic images. It is not inconceivable that a staff member, or a student, at an FE/HE institution might store encrypted or otherwise disguised files containing paedophilic images on the institution's servers to which they have been granted ready access.

It might then be considered that the institution is in possession of those images, contrary to law. However, Section 160 of the Criminal Justice Act 1988 also provides a defence where:

"a person charged with an offence under [this section].... had not himself seen the photograph or pseudo-photograph and did not know, nor had any cause to suspect, it to be indecent"

Internet paedophiles tend to go to some lengths to ensure that their activities are kept secret and their materials remain accessible only to a small group of like-minded individuals. It is therefore difficult to imagine a situation in which this defence would not be available to a FE/HE institution in respect of possession of an illegal image by virtue of it having been stored on its servers.

The availability of this defence does, of course, carry with it an obligation to report child pornography to the police as soon as the institution becomes aware of it.

#### **4.5. Conclusions on liability for obscene or paedophilic materials posted by third parties**

It would seem, then, that liability in respect of pornographic and obscene material which third parties post to an institutions servers is not such a looming threat. However, it will of course require policy decisions in relation to internal disciplinary procedures, and when to involve the police, etc..

It will also provide some reassurance to note that UK policy in dealing with obscene material uncovered on the servers of commercial ISPs has, over the last several years, tended towards the police working with the ISP. This co-operation is an attempt to identify and apprehend the perpetrators, rather than penalise them for possession of the illegal material. The operation of the Internet Watch Foundation, primarily aimed at the elimination of online child pornography is an example - <http://www.iwf.org.uk>.

### **5 Liability for Defamation**

#### **5.1. Introduction**

FE/HE Institutions now often make use of bulletin board systems and newsgroups, either as a facility for students to discuss courses amongst themselves, unmonitored, or as a vehicle for tutorial-style tutor-led discussion.

If these groups are located on an institution's servers, or the institution maintains a sufficient level of control over the system, it must be considered whether the institution is at law a "publisher" of this material for the purposes of defamation. Defamation is, essentially, concerned with the publication of lies, or untruths.

The general rule of UK defamation law is that the publisher of a defamation faces strict liability. When the current legislation, the Defamation Act 1996, was before Parliament, the position of internet intermediaries was much debated. It was accepted that it would be unfair to subject an ISP hosting a newsgroup to the same level of liability as a 'real-world' publisher. The latter has the opportunity to check over all content before it is placed in the public domain (as opposed to a exercising a greater or lesser degree of editorial control over an internet newsgroup to which a large group of persons may post directly).

## 5.2. Defence to liability

Under the Defamation Act (Section 1(1)), an ISP will have a valid defence to the dissemination of a defamation where:

- It is not the "author, editor, or publisher" of the defamation.
- It did not know and had no reason to believe that the statement in question was defamatory
- It took reasonable care in relation to the publication of the statement in question

Further, under Section 1(3)(e), of the Defamation Act 1996 an ISP will not be considered to be the "author, editor, or publisher" of a defamatory statement:

"...if [the ISP] is only involved...as the operator of or provider of access to a communication system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control."

It must be noted that while it provides 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) and the defence in section 1(3). On the one hand 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. On the other hand, 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.

## 5.3. ISP Liability, Defamation and Godfrey v Demon

The first UK case on ISP liability for defamation was Godfrey v Demon (1999) QBD, [1999] 4 All ER 342. This was a preliminary hearing in order to establish whether the ISP could take advantage of the defence in section 1(1) described in 5.2 above.

The facts were that an unknown individual had posted a message to a newsgroup hosted but not actively monitored by the ISP. This message, which contained certain racist statements, claimed to be written by Mr Godfrey, however, this was not the case. Godfrey notified the ISP, Demon, of the existence of the statement. Demon failed to take any action to remove the offending post until the system automatically overwrote it some ten days later. The court found that up until receiving notification of the existence of the allegedly defamatory posting, Demon could not have had sufficient reason to suspect that it was not made by Mr Godfrey. However, from the point that actual knowledge was received, the defence was no longer available.

Due to the nature of defamation, unless the ISP is aware of all the facts surrounding a particular statement, it is often impossible to determine whether it is true. In seeking to determine whether an ISP

took reasonable care in relation to the publication of the statement and had no reason to believe it to be defamatory, the courts are likely in future to look to the nature of the newsgroup.

In this case, Demon had no reason to suspect that postings to a newsgroup about Thai culture (the newsgroup to which the posting in this case was made was entitled soc.culture.thai) would be especially likely to be defamatory. Had the newsgroup instead been entitled 'Scandalous B'stards', with a reputation for and a clear intention to attract postings of a potentially defamatory nature, it is a strong possibility that the court would have found Demon liable prior to receiving notification from Godfrey. The grounds for this are that they could reasonably have been expected to be aware of circumstances likely to render the posting defamatory.

#### **5.4. Implications of Godfrey v Demon for FE/HE institutions**

What implications does this have, then, for newsgroups and bulletin boards run by FE/HE institutions?

With respect to unmonitored newsgroups, hosted on an institution's servers, and not actively monitored, the institution will be able to take advantage of the defence in section 1 of the Defamation Act.

Where there is neither actual knowledge of the defamation nor awareness of any facts or circumstances from which the institution could reasonably have been expected to be aware of the defamation, and the institution has taken reasonable care in relation to publication of the statement in question, the defence is likely to be open. Upon receipt of notice of a claimed defamation, the institution should, of course, remove the posting complained of immediately.

#### **5.5. Defamation, Liability, and Data Protection**

The facts in Totalise plc -v- Motley Fool Ltd (2001) were of a similar nature to those in Godfrey -v- Demon. Motley Fool, unlike Demon, responded rapidly to notification of the defamatory postings made under the screen-name "Z Dust", removing all postings corresponding to that individual and revoking his access to the newsgroup on the same day as notification was received.

The plaintiffs applied for a court order which would require the ISP to provide information in its possession which could lead to the identification of the poster (for example, details of the IP address of any computer which "Z Dust" had used in order to access and post to the newsgroup).

The ISP declined to hand over any such information on the basis that this would be in breach of its privacy statement and/or data protection legislation. The ISP claimed that it was entitled to make such a refusal as the plaintiffs intended to use the requested information as a basis on which to seek legal advice. They also claimed that such a "fishing expedition" was insufficient justification for a breach of data protection and privacy. The court found, however, that as "Z Dust" had waged an intensive campaign of defamation against the plaintiffs, a tort had clearly been committed and the only obstacle to the bringing of an action was the inability to identify "Z Dust".

The court further referred to Section 35 of the Data Protection Act 1998. This section provides an exemption from the non-disclosure requirements in respect of personal data where:

"(1)...the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

(2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary-

(a) for the purposes of, or in connection with, any legal proceedings (including prospective legal proceedings) or

(b) for the purpose of obtaining legal advice,

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights."

The court therefore found that it was not necessary that the plaintiffs be committed to an ongoing legal action in order to be able to require disclosure under Section 35.

The defendant ISP also sought to rely on Section 10 of the Contempt of Court Act 1981. However, the court found that this section (which provides that a party cannot be held in contempt of court for refusing to disclose its sources of information, save where such disclosure is required "in the interests of justice or national security or for the prevention or detection of disorder or crime.") was intended only for the protection of a journalist's sources. This protection against disclosure was found not to be open to an ISP which did not take responsibility for information posted to its newsgroups.

This case confirms that an ISP - or a FE/HE institution in these circumstances which acts with all due haste, once notified, to remove defamatory postings from its servers, and complies with such request for information which may identify the poster, will not face liability in respect of the defamations.

## **5.6. Defamation, Liability, and On line Discussion Groups**

Difficulty arises in relation to discussion groups which function as online tutorials, monitored by a member of the institution's teaching staff.

The level of control exercised over such groups is of relevance. Typically, access will be limited to a small number of participating students and the tutor, with all answers being read and commented upon by the tutor.

In such a situation it is highly likely that the institution would fall within the remit of "editor", or "publisher", and thus not be entitled to rely upon the section 1 defence. This raises obvious problems, remembering that where sufficient editorial control is present, the institution becomes strictly liable for the content of the newsgroup / bulletin board.

The closed nature of the tutorial group makes no difference, as 'publication' of a defamation requires merely disclosure of the defamatory statement to one person other than the subject. This would seem a harsh approach for the courts to take in relation to an academic institution (as opposed to, for instance, a frivolous tabloid newspaper), but it would seem to be the only logical interpretation of the law in this context.

It should, however, be remembered that any defamatory remark posted to a closed tutorial group is more than likely to be 'off-topic', and it should be a fairly simple matter to ban such posting and to delete messages not relevant to the discussion as a matter of course.

The ease with which a student in a closed tutorial group can be identified (not to mention any internal disciplinary procedures and penalties) should act as a strong deterrent to the making of defamatory posts.

It then becomes a matter of taking all reasonable steps to ensure the security of the system in order to prevent anyone not properly authorised from posting to the group.

## **6 Liability for third-party copyright infringement**

### **6.1. Introduction**

The online world raises many well-documented issues in relation to copyright. These include, for instance, deliberate student plagiarism of journal articles and essays available on the web, as well as inadvertent infringement, as, for example, where a staff member copies large chunks of an online text to use as part of a pack of teaching materials.

Where staff and students have been provided with accounts and storage on an institution's network, infringing copyright material can also be stored on the institution's servers. The development of peer-to-peer file sharing software, such as the notorious (and now defunct) Napster, or Morpheus, KaZaA, and the others which have arisen to take its place, has given rise to much copyright infringement in the trading of copies of (mostly, but not exclusively) mp3 audio files.

The high speed, broadband internet access typically available via a FE/HE institution's network, allowing larger file formats to be downloaded much more quickly than via home-dial-up accounts, is a highly attractive facility with which to use these file-sharing systems. Students and staff members can very

easily download the peer to peer software to their account on the institution's network and use those to store a large quantity of information, much of which is likely to be infringing.

## 6.2. Secondary copyright infringement

It is a possibility, then, that at any one time a large quantity of copyright infringing material could be stored on a FE/HE institutions servers. Does this mean that the institution will incur liability in respect of this infringing material? Under Section 23 of the Copyright, Designs & Patents Act 1988, 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. This is known as secondary copyright infringement. To deal with the first element, it is highly improbable that a FE/HE institution would qualify as being in possession of the copyright infringing material in the course of a business. (The Act, in section 178, which deals with "minor definitions", defines "business" as "includ[ing] a trade or profession.") Even if this were held to be the case, the knowledge requirement would be very difficult to pin down.

Actual knowledge of an infringement is a simple issue, and any potential liability can be easily sidestepped by simply deleting infringing material from an institution's servers as soon as is practicable once notified or otherwise made aware of its existence.

The boundaries of constructive knowledge ("reason to believe"), however, are somewhat blurred. In the online environment, there is a high likelihood that infringing copies will be present. An example of this would be mp3 files traded over a peer to peer system and stored on the institution's servers.

The question arises whether such constructive knowledge is sufficient for a finding of liability on the part of the institution. 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 in the 1988 Act, 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* ([1982] FSR 565), 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* ([1987] ChD 38), it was held that a general knowledge that some copies may be infringing did not constitute sufficient knowledge for secondary copyright infringement.

At present there seems no reason to doubt that the courts will place a similar interpretation upon the same provision in the 1988 Act. If this is the case it would appear highly unlikely that a FE/HE institution could face liability for secondary copyright infringement.

## 6.3. Copyright Directive

Amongst other provisions 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" (Article 2), the "right of communication to the public" (Article 3), and the "distribution right" (Article 4). 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 (see Article 5, which deals with a long list of exemptions for various contexts).

It must also be remembered that the exemptions from liability provided in the E-commerce Directive will work in conjunction with this Copyright Directive. The purpose of this being to ensure that ISPs are not unfairly exposed to heavy liability for third party provided content (see discussion of the Electronic Commerce (EC Directive) Regulations 2002, at 6.4).

FE/HE institutions will be able to take advantage of these limitations also in respect of material passing through and stored on their servers.

At time of writing, the UK Patent Office is undertaking a consultation process with respect to implementation of the Copyright Directive. The consultation document includes a number of draft amendments to the Copyright Design & Patents Act, all couched in very much the same terms as the language of the Directive, and designed to give effect to the latter's minimum requirements.

#### **6.4. Electronic Commerce Regulations**

The bounds of ISP liability for third party provided content under UK law have now been further clarified by the passage of the Electronic Commerce (EC Directive) Regulations 2002.

These regulations enact the Electronic Commerce Directive, and include several provisions which restrict ISP liability in certain cases. As discussed above, the relevant parts of the Regulations apply to the "service provider" of an "information society service". These terms are defined such that an FE/HE institution offering internet and storage services via its servers to staff and students will fall within their ambit. There are four main regulations at issue here.

##### **6.4.1 Mere Conduit**

Regulation 17 is concerned with the situation in which the ISP is a "mere conduit" i.e. a pass-through provider which merely passes on information provided by a third party, or provides access to a communications network.

The definition of "Transmission" includes "automatic, intermediate and temporary" storage of any information transmitted so far as this occurs "for the sole purpose of carrying out the transmission", and does not continue for any longer than is strictly necessary to facilitate transmission.

Where this is the case, the service provider will not face any form of liability, civil or criminal, in respect of the content of the transmission, provided that the following conditions are met:

- The transmission was initiated by a party other than the service provider - e.g. a student using a FE/HE institution-provided internet access account
- The service provider did not select the recipient of the transmission - e.g. the institution's network was used by a student or a staff-member to send an email to a third person selected by the sender
- The service provider did not "select or modify" i.e. alter or tamper with, the content of the transmission (e.g. an email) in any way

Thus a FE/HE institution will not face liability in respect of an email sent via its system (subject to the system's meeting the Regulations' requirements on "transmission"), despite any defamatory, copyright infringing, obscene or otherwise illegal content.

##### **6.4.2 Caching**

Cached content under the Regulations is information which is:

"the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request..."

Cached information usually takes the form of a temporary copy of a recently visited website, stored locally to facilitate more rapid access by the user.

Regulation 18 provides immunity from liability for ISPs in respect of information which may be cached on their servers. For example, should a student or member of staff cause a copy of an obscene website, or one containing defamatory statements, to be stored on a FE/HE institution's servers, the institution cannot be held liable in respect of that illegal content.

This immunity is subject to similar conditions as the transmission immunity. It applies where the service provider:

- Does not modify the cached information
- Complies with access conditions in relation to the information
- Complies with any rules (e.g. recognised industry standards) in respect of updating the information
- Does not interfere with the lawful use of technology with the intention of obtaining data on the use of the cached content

Under Regulation 18 there is a further obligation placed upon ISPs in relation to cached content, which goes beyond simple requirements stipulating how the system must operate in order for the immunity to be available.

This is when an ISP receives "actual knowledge" of the fact that information has been removed at the original source, or access to it there disabled, or that such removal or disablement has been ordered by a court or an administrative authority.

The text of the original Directive to which these Regulations give force in the UK was much criticised for the lack of any definition of what exactly constitutes notice with regard to "actual knowledge". The Regulations do, however, provide some indication as to the scope of such notice

#### **6.4.3 Actual Notice**

Regulation 22 provides a non-exhaustive list of factors which a court will consider in determining whether actual notice has been issued to the service provider. These include whether the service provider has received a notice through any means of contact that the service provider has made available in compliance with regulation 6(1)(c).

Regulation 6(1) requires the service provider to make certain information available to the user "in a form...which is easily, directly and permanently accessible". Regulation 6(1)(c) refers to contact details of the service provider, including email addresses, which permit rapid and direct communication. This requirement can be easily fulfilled by placing an obvious link on an institution's homepage which points to email, telephone and other contact details. A dedicated email address for dealing with complaints may be helpful, provided that it is checked at least daily for incoming mail.

Other factors which a court should consider under Regulation 22 are:

- "(b) the extent to which any notice includes -
  - (i) the full name and address of the sender of the notice;
  - (ii) details of the location of the information in question; and
  - (iii) details of the unlawful nature of the activity or information in question."

It would be wise to treat any complaint email / telephone call etc which on investigation proves to be genuine, (i.e. the content complained of is indeed on the servers, and the service provider is not the recipient of a prank) as constituting actual notice. In practice, this may help to protect the FE/HE institution from liability as the service provider.

#### **6.4.4 Qualified Immunity**

Probably the most significant of these provisions on ISP content liability is regulation 19, which provides a qualified immunity for ISPs in respect of third party provided material hosted on the ISP's servers. This immunity, which again applies in respect of both civil and criminal liability, is subject to the following conditions:

- The service provider has no actual knowledge (as 6.4.3 above) of the content in question. Once the service provider is in receipt of actual knowledge of the illegality, it must act to remove or disable access to the material as quickly as possible.
- The service provider is not aware of facts or circumstances from which the illegality of the content in question should have been apparent

- The user responsible for providing the content in question was not "acting under the authority or the control of the service provider" - an employee of a university putting the information on the server in the course of his employment, for instance.

In most cases, a FE/HE institution staff member or student will not be acting either in the course of his or her job or with the authority of the institution by posting illegal information to the servers - for instance, placing obscene material online, or posting a defamatory message to a bulletin board.

These conditions essentially apply an intermediary liability standard in respect of all third party provided content that is the same as that already extant for defamation under section 1 of the Defamation Act 1996.

Godfrey -v- Demon and Motley Fool -v- Totalise plc, remain strictly speaking, cases decided in the main under the defamation legislation and thus not directly applicable as precedents elsewhere.

In respect of obscene material, or copyright infringement, these cases do however give some indication as to how the limited immunity for liability for third party provided content, might be applied by the courts.

As required by the original European Directive, the Electronic Commerce Regulations impose no general duty to monitor for illegal content. However a service provider foolhardy enough to wish to adopt further responsibility than that proscribed by regulations 17, 18 and 19 may do so under regulation 20(1)(a), which provides that nothing in the preceding regulations shall "prevent a person agreeing different contractual terms." Of course, it would be highly inadvisable for any FE/HE institution to do so.

## **7 What is to be done?**

FE/HE Institutions can significantly reduce the risk of liability for third party content by adopting the following strategies:

- Acceptable use policies (AUPs), drawing particular attention to unacceptable conduct and content in relation to internet service facilities, should be drawn up by the institution and complied with by all users. The JANET AUP should form the core of any such code which an individual FE/HE institution adopts. All staff and students should be required to indicate their agreement to be bound by the AUP as part of the process of registering for online services. It may also be a good idea to set up communal access terminals (in libraries, student computer rooms, etc) such that a window containing the AUP is always displayed upon log-in.
- The AUP should incorporate a clear 'notice and take-down' procedure for reporting unacceptable content on the College or University servers. This should include contact details for the relevant office or person who should be notified. Of course, this will require to be backed up by clear administrative procedures for dealing with complaints quickly and efficiently.
- For any AUP to be effective, it will require to be supported by a clear internal disciplinary system. This will need to include some indication as to what matters will be dealt with purely internally. As an example, an institution may decide that its network resources should not be 'wasted' by staff or students wishing to use the facilities just to look or store pornography. Where a user is found to be in violation of this by accessing or storing otherwise legal pornographic content, this would be grounds for internal disciplinary action. Should the material be child pornography or otherwise obscene, it will be necessary to involve law enforcement. Clear guidelines need to be in place as to when the police will be involved. The penalties for a violation of the AUP should also be made clear.
- It may be desirable to include in the AUP some form of limitation of liability clause whereby the user agrees to indemnify the institution against any liability incurred as a result of the actions of that individual. This will not prevent the institution from incurring liability in the courts. However, should this happen it will, assuming the clause is not 'unfair' under the terms of, for example, the Unfair Contract Terms legislation, entitle the institution to sue the user for recovery of any damages paid out. While in practical terms an individual student or academic is highly unlikely to have the economic resources to meet such a claim, this may help to impress upon users the importance of adhering to the rules regarding the use of institutional internet facilities.

- It is advisable only to offer website hosting facilities to staff members for work purposes: If students are enabled to set up their own personal webpages on University servers, the risk of incurring liability in respect of copyright infringement, for example, will be higher.
- It may be desirable to block access to certain websites - for example, certain sites known to be sexually explicit, or sites which offer peer to peer software, such as Audiogalaxy or KaZaA, for download. This would cut the risk of individuals using network storage facilities for obscene or copyright infringing material. What institutions must not do is to adopt a policy of general monitoring of their servers and/or user accounts. By adopting such editorial control an institution can open itself to liability as a publisher under the Defamation Act, or, in relation to content more broadly, may put itself in a position where it could be considered that due to a policy of active monitoring it should have been aware of certain illegal content which has 'slipped the net'.
- With regards to bulletin board systems and discussion groups on an institution's servers, it may be sensible to, as far as is possible, restrict these to groups to which only a limited number of registered students may post (for instance, the members of a particular class or tutorial group) These should only be accessible via registered accounts in order that all posts are traceable to the author. This may, as discussed above, open the institution to a potentially higher liability standard. However, this will be heavily mitigated by the fact that it is highly unlikely that a genuine tutorial response will contain anything illegal - such posts are more likely to be off-topic, and all off-topic posting can be eliminated relatively easily. It is also a rare student that will risk breaking the rules regarding posts when they are readily identifiable by their user ID and thus easily disciplined.
- Contact details for the person or office in charge of dealing with complaints about material on an institution's servers should also be provided via a clear link on the institution's homepage
- With respect to complaints received regarding potentially illegal content, any direct contact should be treated as 'actual notice'.
- 'If in doubt, take it out' - where the legal status of content (is a statement defamatory? Is this an infringing copy? Is this material obscene?) is in question, it is always wiser to remove it from the servers rather than risk occasioning liability as did Demon in Godfrey -v- Demon. In some cases, however, such as suspected child pornography, while the material must be made inaccessible as a matter of urgency, it would be wise to contact the police before deleting completely in case it is required in evidence.

ISP liability for third party content is a potential minefield - and one which FE/HE institutions providing internet facilitated to students and staff must cross. However, with due care and attention, following the guidelines above, it is possible to minimise liability sufficiently that it need not be the looming threat it may at first appear.

Author Gavin Sutter LL.B. LL.M. Institute for Computer & Communications Law  
Centre for Commercial Law Studies University of London g.sutter@qmul.ac.uk

10 June 2003

© JISC Legal Information Service