Judge and Jury ?

how "Notice & Take Down" gives ISPs an unwanted role in applying the Law to the Internet.

Written by: Richard Clayton, Internet Expert, Thus plc
richard@demon.net

26th July 2000†

Summary

The widely reported out-of-court settlement of the defamation action *Godfrey v Demon Internet* in favour of the physicist Dr Laurence Godfrey has ignited a debate as to how far Internet Service Providers (ISPs) should be responsible for material on the Internet.

Many UK laws are such that the safest thing that ISPs can do is to "take down" material once put on "notice" that it may be unlawful. This can lead to injustices as lawful material is censored because ISPs cannot take the risk that a court will eventually agree that it can indeed remain available.

The authors whose material is "taken down" by an ISP will increasingly be looking at their own legal rights. As ISPs seek to insulate themselves from actions for breach of contract, their terms and conditions will appear more and more arbitrary to potential customers, who will increasingly look abroad for services such as web hosting.

This paper gives an account of recent events and discusses the rapidly increasing level of complaints already being received by ISPs. Several legal frameworks are reviewed, particularly the situation in the USA, where ISPs enjoy considerable immunity.

Two particular legal solutions to the problems faced by ISPs are then examined:

The first possible solution is blanket immunity for ISP activities. This has obvious attractions for the industry, since the only need is to act on orders made by the courts. It will, however, increase the general cost and complexity of removing disputed material from the Internet.

The second proposed approach is a new statutory regime that would cover not only defamation but also a range of other issues. It strikes a balance between complex burdens for ISPs and prompt responses to complaints that harm is being done. It is designed to be "lightweight" and in very many cases it may operate without the courts becoming involved at any stage. It works in a similar way to USA's Digital Millennium Copyright Act's approach to copyright infringement. The proposal is designated "**R4**", and works as follows:

Report	- a complainant serves a notice of infringing material
Remove	- the ISP removes it, without judging the merits
Response	- the author can contest this by asking for replacement
Replace	- again the ISP acts automatically

The key legal protections provided by both solutions would be that the ISP is not liable to either complainant or author if they follow the process; and, as a safeguard for all concerned, malicious or negligent claimants can be penalised by the courts.

The public policy result of either solution would be that certain aspects of UK law could be applied on the Internet without having to co-opt the ISPs to become "Judge and Jury".

† Some draft versions of this document were widely circulated in May 2000. The main difference in this final version is that it is now suggested that within the R4 scheme, the courts should always be involved before anonymity is lifted from an author.

Godfrey v Demon Internet

The recent out-of-court settlement of two *Godfrey v Demon Internet* defamation cases has been seen by many commentators as a landmark in the application of the law to the Internet. However, this shows a poor understanding of the actual issues and of the history of the subject. In fact, the details of the case make it of limited relevance and the key judgment was made over a year ago.

This was not even the first "Internet libel" case in the UK, that "honour" going to *Laurence Godfrey v Philip Hallam-Baker* which related to events in 1993 and was settled in 1995. Neither was it the first time an Internet Service Provider (ISP) has been taken to court in the UK. Dr Julian Lewis MP sued Demon Internet over a Scallywag web site in 1996 and Dr Godfrey has previously issued writs against Australian, New Zealand, Canadian and American based organisations.

However, *Godfrey v Demon Internet* has been one of the most widely reported actions. Two cases were settled on the 30th March 2000. They differ in some of the details.

The first case relates to events in January 1997 when an unknown user of an ISP in Ohio, USA forged a "Usenet" article in the name of Dr Laurence Godfrey. The article was "squalid, obscene and defamatory". Dr Godfrey immediately posted articles to Usenet denying that he was the author and tried, and failed, to persuade the Ohio ISP to reveal the identity of the forger.

Usenet works by distributing articles to hundreds of thousands of local servers where they will be preserved for a week or two for customers to read. After that time they "expire" and are deleted, though some systems may archive them for longer-term access. A few days after the article had been posted, Dr Godfrey became aware that the article was still available on Demon's news service and requested its removal. Demon took no action. When Dr Godfrey's solicitor wrote formally, the article had already expired from Demon's service, but Demon made no response to the letter. Dr Godfrey issued a writ in January 1998. In a March 1999 pre-trial hearing Mr Justice Morland struck out parts of Demon's proposed defence under Section 1 of the Defamation Act.

The second case relates to events in the summer of 1998. A user of an anonymous posting service published articles in several newsgroups that made defamatory claims about Dr Godfrey's personal life. These articles were almost immediately cancelled so that they were no longer available. However, whilst they were still available a Demon Internet customer retrieved a copy and re-posted the remarks along with some sardonic commentary of his own. Dr Godfrey asked for this article to be removed and cancelled, but Demon did not act.

The first case was settled for a payment of £5,000, the second for £10,000. Dr Godfrey's costs (said at the time to be of the order of £230,000) are to be paid by Demon.

The Defamation Act 1996

As can be seen from the facts set out above, legal action would not have succeeded if Demon had acted upon Dr Godfrey's requests. Section 1 of the Defamation Act protected them before these requests arrived. However, Demon did not act when the requests were made and then sought, in effect, to claim that because of the automatic and hands-off operation of their news server Section 1 of the Defamation Act 1996 continued to excuse them from liability. Mr Justice Morland held that this was "in law hopeless" and struck out this part of their defence.

It should be noted that there are some special definitions of “author”, “editor” and “publisher” in the Defamation Act – they do not quite have their everyday meanings. Under the Act, Demon was not a publisher, but failed to meet the other tests in Section 1(1) since they had been put on notice of the existence of the defamatory material. In other words, they could no longer claim “innocent dissemination”.

The other defences available under the Act of just being the printer or transporter of the material were not applicable. The crucial issue was the amount of potential control over future publication. Although news server operation is usually automatic, it is possible to manually override article retention if required.

The operation of the Defamation Act is usually described as a “notice and take down” regime. ISPs have substantial protection until they are put on notice. When the “notice” is served they must promptly “take down” the material to avoid liability.

ISPs as judge and jury

When articles are clearly defamatory “notice and take down” is very simple to operate. However, in practice, those who do not have trained legal minds will find that cases are seldom clear. Therefore, an ISP is very likely to have to incur the expense of getting a formal legal opinion before deciding if an article needs to be removed. “Vulgar abuse” will not be held by the courts to be defamatory – but expert advice may be needed in order to distinguish the nature of a particular example of invective.

> This expert advice may be surprising to those who are used to seeing “flame wars” on Usenet. For example if one poster says “are you another of those unwashed work-shy social security scrounging wankers” and the other replies “is clueless and groundless bigotry your forte?” then this goes beyond abuse and both have defamed each other.

Having received expert advice and removed the defamatory material the ISP’s problems are far from being at an end. The author may admit the defamation but claim justification – what they said was true – and require that their contract with the ISP be honoured and their material be reinstated.

> For example if a poster writes that a radio station misreported the *Godfrey* case by referring to a “chat room” rather than “Usenet” then this can, in context, defame the radio station by suggesting that they have made a basic and stupid mistake. It should be noted that much of the media reporting of the *Godfrey* case was inaccurate in its details, but if the particular broadcast is not available for review, it is impossible for the ISP to know whether the poster is giving an accurate account of what they heard.

Some obvious questions arise and the answers are currently completely unclear:

- To what extent should the ISP assess complaints to determine if material is unlawful by checking the material and the legislation? Is common-sense enough, or should a formal opinion be sought from a barrister in the Temple?

- Should the ISP be seeking proof from the complainant that legal action is contemplated? The Defamation Act allows third parties to put the ISP on notice. Is there any duty on the ISP to take steps to identify the complainant? let alone their intention to sue?

- Is an ISP ever entitled to conclude that a claim is trivial and ignore it?

- Should the ISP hold a private trial to decide on “justification”?

- To what extent would any quasi-judicial procedure adopted by an ISP be open to challenge under the European Convention on Human Rights ? The ECHR is already part of the law in Scotland and will be extended to the rest of the UK in October 2000.

- If the ISP seeks a legal indemnity from the author and reinstates the material, what then is their position if the author is a “man of straw” and the indemnity is worthless?

- If the author promises future good behaviour then has “reasonable care” been taken by any ISP who thereafter offers the author access to the Net? What if the author refuses to give any promises to one ISP and then becomes a customer of another?

The most immediately obvious result from the March 1999 ruling was a substantial rise in the number of complaints being made to ISPs. The most obvious result of the March 2000 settlement was that this turned into a flood. In one week in early April Demon received more complaints than in the entire previous history of the company.

The expense of judging these complaints in a fair and consistent manner is clearly substantial and, as indicated above, might well be open to challenge under Human Rights legislation.

One must expect to see ISPs, particularly those who are providing low-margin services, starting to take the view that it is too expensive to be “right” and that automatic action upon complaints, whatever their merits, will be rather more cost-effective. This can rapidly lead to “denial of service” attacks upon ISPs as complaints of dubious merit are made and a substantial amount of material is removed under automatic procedures.

Of course defamation is not restricted to Usenet. There are, if anything, more complaints being made to ISPs about web sites – particularly as people start to use the new medium for campaigning. Problems have occurred with sites dealing with miscarriages of justice and attempts to discuss the operation of local councils’ social services and planning departments. Since the ISPs will never be in a position to decide whether a campaigning site is actually telling the truth – and charges of maladministration are far more serious than the name-calling discussed above – when complaints are made, it is inevitable the site will be removed.

ISPs will need to guard themselves against the liability that would arise if the campaigners turned out to be right – and hence the site was not unlawful. Therefore, the ISPs will be increasingly adding clauses to contracts that allow them to act almost arbitrarily to remove material; going as far as the ‘Unfair Terms in Consumer Contracts Regulations’ will permit.

This type of contractual clause, which allows ISPs to dictate what cannot appear on websites, will be inherently anti-consumer and cannot therefore be in the wider public interest.

The clauses will also affect sales. Legitimate customers will see the potential effect upon their own investment in an online presence as unfair or unreasonable. They will be dismayed to find that ISPs must protect their own position and these terms cannot be negotiated away. There is a considerable risk that business will be tempted offshore where web-hosting services do not have such apparently one-sided provisions.

The Defamation Act must be welcomed as moving beyond “strict liability” regimes that make ISPs liable for content even when they are completely unaware of its presence. However, when the ISP is made aware, perhaps by a third party and not by the person who is defamed, then the practical problems are considerable and were clearly not properly thought out when the law was last changed.

Common Carriers

Some people have argued that ISPs need to become "common carriers". This is confusing because in UK common law the carriers accepted full liability (with appropriate insurance) for what they carried – but they could refuse some material up front. The term as applied to US telephone companies means that they get immunity from what they carry, provided that they carry everything they are requested to.

Some people think that the Royal Mail is a "common carrier" but in fact section 7 (4) of the Post Office Act 1969 states: "The Post Office shall not be regarded as a common carrier in respect of any of its activities". The immunity that the Royal Mail does enjoy comes from elsewhere in the Act where, in a US style scheme, there is a trade-off between universal service and exemption from liability.

The ISP industry is not, in its current stage of evolution, ready to offer any form of universal service guarantee. Without that, there is not the traditional "quid pro quo" for granting widespread immunities under a "common carrier" approach.

What is special about ISPs ?

Now of course all of the problems that the "poor unfortunate ISPs" have with defamation are exactly those problems that have been faced by book publishers, high street newsagents, magazine publishers (and even Golf Club notice-boards!) for decades. However, there are some very important differences.

The first is one of scale. Literally millions of people are now creating content on the Internet and that material can be seen by tens of millions. The lack of filtering by professionals before publication makes defamation several orders of magnitude more likely to occur than in traditional media.

The second difference is the equality the Internet provides. Individuals defamed on the Internet will often have similar access to those people who saw the original material and can not only rebut the defamatory statement, but they can do this almost immediately. This differs from the conventional situation where publishers and broadcasters may have to be compelled to publish a retraction, which can be much delayed and is invariably far less prominent.

The third and most important difference that the ISPs experience is one of global competition. W.H. Smith operates under the same legal regime as Waterstones, but placing web sites on the other side of the planet, where ISPs are immunised against their customers' actions, is just as easy and effective as hosting them at the centre of the UK Internet industry in London's Docklands. If placing web sites in the UK comes to be seen as problematic compared with hosting them in the USA, there is very little to prevent a significant proportion of this business from going offshore.

Copyright and other laws

This paper has, so far, been concentrating on defamation – but this is just the tip of a very large legal iceberg. Copyright infringement and other misuse of Intellectual Property is extremely widespread and once again the ISP must act as "Judge and Jury" to decide the merits of a case.

If Disney complains that a website contains an unlicensed image of Mickey Mouse then it may be easy to make a decision. What if (and Demon report this as a real life case) two lingerie companies each counterclaim that a photograph of model wearing their goods is their property and the other is infringing. The ISP has a 50/50 chance of making the right decision, and if the wrong decision is made then there will be considerable damages to be paid for both continuing to publish the image and for removing a website for no valid reason.

Even where ISPs spend the effort (and considerable expense) in assessing the merits of a case, if the dispute eventually ends up in court there is no immunity for the ISP from the consequences of having made an incorrect interim decision. Documents may be produced that the ISP never saw, or the court may take a different view of the validity of the key pieces of evidence. Furthermore, even if the ISP does come to the correct decision, whether or not it is endorsed by the court, there will be an inevitable delay whilst the ISP's quasi-judicial procedure takes place. This delay may of itself, considerably increase the damage that has been done by the appearance (or removal) of the material.

Besides a whole raft of civil issues, there are some criminal offences that can be committed by publishing material – sedition and blasphemy may not be fashionable, but they are still on the statute book. Looking at more modern concerns, it is also possible to commit offences under the Race Relations Act and indeed publishing instructions on marijuana cultivation or the synthesis of LSD are unlikely to be lawful (prosecutions for "incitement" to grow cannabis have succeeded in the past).

Although whether or not to leave material visible on the Internet whilst a prosecution was pending might seem an easy decision, there will always be complexities, especially when the Internet aspects of the case are tangential to the actual criminal charges.

The ISP industry has addressed one particular criminal issue, that of publishing "child pornography", by setting up the Internet Watch Foundation (IWF). This body acts as a clearinghouse for the industry, operating a hot line for the public and doing some proactive scanning of areas where the material is common. It uses its expertise to determine if images are illegal and advises ISPs accordingly as to whether material needs to be removed. The ISPs act on the expert opinion encapsulated within these removal notices.

There have been few complaints about this type of removal, since in this type of case the author is invariably more interested in trying to escape the attentions of the Police than in disputing with the experts as to whether borderline material should have been removed.

The industry and successive Governments have perceived the IWF to be an effective way of dealing with a complicated problem, but it is not cheap to run. Its expertise is based on making objective tests about the legality of material that do not require external evidence.

The ISP industry would not welcome the extra financial burden of funding further centralised bodies to address other issues such as defamation or copyright infringement. The expense would be considerably more than the IWF, since unlike expert opinions on the legality of images of children, the decisions could not be made in isolation but would often require complex investigations to be conducted.

The IWF is finding it a challenge to widen its funding base. It is far from clear that any other, inherently far more expensive, types of centralised body would find it at all simple to raise the money needed to operate.

The law in the USA

The USA grants substantial immunities to ISPs. In particular, the **Telecommunications Act** of 1996 230(c)(1) provides that in many circumstances "*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 probably worth noting in passing that this 1996 law originally included (as Title V) the provisions of Senator Exon's **Communications Decency Act**. Much of this attempt to regulate content on the Internet was struck out by the Supreme Court in June 1997 as an unconstitutional attempt to restrict First Amendment free speech rights. However Section 230 remains on the statute book.

The law has been upheld in *Zeran v AOL*. Shortly after the Oklahoma City bombing, an unknown person posted messages onto an AOL bulletin board falsely implicating Zeran. He filed a lawsuit against AOL for the allegedly defamatory postings, claiming that AOL was unreasonably slow in removing the messages. The courts held in favour of AOL, because Section 230 protected against liability for defamatory information posted on the network by someone else and for any negligence in failing to remove that information.

Lest it be thought that Mr. Zeran did not receive justice, it is worth reviewing the related case of *Zeran v Diamond Broadcasting Inc* where the AOL messages had been discussed on a breakfast-time radio show. The court held that Zeran had suffered little actual damage and had applied the principle of *de minimus* (i.e. that the law is not concerned with trifles) in dismissing the case.

This summary of Zeran necessarily skips many details – and in particular it should be noted that the law on defamation in the USA is very different from in the UK. The full text of the judgments can be located at:

http://legal.web.aol.com/decisions/dldefam/zeran.html

The law in the USA that deals with copyright issues on the Internet is the DMCA **(Digital Millennium Copyright Act** 1998 Title II). This legislation provides several clear schemes to protect Online Service Providers (OSPs) and network operators. There are specific immunities for transitory digital communications and for "caches" that provide "automatic technical processes" for local storage of material to reduce bandwidth costs.

For the current discussion, the most interesting part of the DMCA is the way in which copyright infringement by OSP customers is dealt with. The Act provides for a "notice and take down" regime within which the OSP does not decide upon the merits of a notice but has merely to act upon it. The law also describes a "counter notification" that can be used by the author of material to have it replaced. Again the OSP has no freedom of action but merely obeys the notice. The process does not iterate; if the replacement is unacceptable to the original notice-giver then the dispute moves into the courts.

There are provisions within the Act to penalise untrue statements made in a removal notice. In order that notices can be easily served there are requirements on the OSPs to register a notice-serving address and to publish this upon the OSP web site. It is also possible for a complainant to obtain the real world address of the person who placed the copyright material onto the Internet, though this involves taking action through the federal court system. The OSP must also meet some technical provisions and, finally, must have a published policy of terminating the access of repeat offenders.

The main feature of the Act from the OSP's point of view is that there is no requirement upon them to make any qualitative decisions. Provided that they follow the rules, which are a bit complex, but nevertheless clear, then they are immune from legal action by any party. The givers of notices can achieve a rapid response, but are accountable before the courts for their actions. In the case of dispute the material will be replaced online whilst the dispute is settled unless the dispute has already come before a court.

The requirement to register has come under fire both as being too bureaucratic and as causing potential problems to OSPs who were unaware of their new obligations. The promoters of the act believed that only a few hundred OSPs would need to register, but in practice more than six thousand have already decided that the Act applies to them.

Some of the other detail in the DMCA can also be criticised, but it is a reasonably fair scheme overall. The clarity of the detail and the direct applicability of the procedures are testament to the close involvement of the American ISP industry in drafting the legislation. The effect of the Act is keep the OSPs out of the central dispute, but to involve them in removal actions as being the quickest and most effective way of ensuring that copyright infringements do not remain publicly available any longer than necessary.

There are reviews of the meaning of the Act on many websites, for example:

http://www.arl.org/info/frn/copy/osp.html

and the full text can be found at:

http://www.dfc.org/assets/images/2281enrolled.pdf

The European Electronic Commerce Directive

The European Union has agreed a **Directive on Electronic Commerce**, which was finalised in early May 2000. It must be implemented under UK law by 2001.

http://europa.eu.int/comm/internal_market/en/media/eleccomm/com31en.pdf

Article 12 of the Directive provides for a defence of "mere conduit" to protect network providers who are simply shifting packets around. Article 13 provides an exemption from liability for information held on caches that store information locally to avoid the expense, and delay, of continual fetching of data from its original remote site. The exemption does require that the caches are operated in accordance with the industry's usual standards. This means that changes to the remote site – perhaps to remove questionable material – will be reflected in the cache contents in a reasonably timely manner.

Article 14 of the Directive on "hosting" requires member states to protect ISPs from liability where they are unaware of the content of information stored on their systems. It further provides for a "notice and take down" regime, without specifying the details of how this should actually be implemented. Finally in this part of the Directive, Article 15 makes it clear that there is no general obligation on service providers to monitor for illegal activity.

For whatever reasons, the Directive does not address any of the practical issues surrounding "notice and take down" regimes such as are discussed in this document. There is no provision on the form of the notice that is to be made nor is there any view as to whether the service provider will have to form an opinion upon the legality of the information before acting on the notice. Importantly for "free speech", there is no discussion of how a notice may be countered by the provider of the information if they feel that they have not broken any laws in making it available.

This lack of detail in the Directive makes it likely that different member states will take different approaches to implementation and hence a "level playing field" will not be established across Europe. However, it does leave it open to the UK Government to frame sensible and relevant legislation to provide significant protection to both ISPs and individuals, as will now be discussed.

Full Immunity

The ISP industry would be happy to receive a "Section 230" style "Zeran" immunity for the actions of others. Clearly, this immunity should not extend to the corporate activities of the ISP itself – but if material originates from a customer or from somewhere else on the Internet then there is obvious merit in giving complete protection to the ISP from something that was outside of their control. The legislative regime would be that an ISP need only act on the instructions of a Court, ie the Electronic Commerce Directive would be implemented by, in effect, severely limiting the form of "notice" that would be required before any "take down".

The downside of a full immunity regime would be that the removal of content from the Internet would become an expensive procedure for the companies and individuals who wished to remove such content, since the courts would always have to be involved.

It might not be appropriate for individuals to have to seek an injunction to request the removal of material posted in the heat of the moment, when the author – once contacted – might well be happy to reconsider their words.

Report, Remove, Respond and Replace ("R4")

The "R4" scheme is intended to strike a different balance from full immunity between placing complex burdens upon ISPs and providing for prompt responses to complaints that harm is being done. It is intentionally designed to be "lightweight" and in very many cases it may operate without the courts becoming involved at any stage.

The scheme is presented as a series of steps with commentary as appropriate. It is envisaged that the procedure would apply not only to all civil actions, but also to criminal matters where it would be usual for the police to issue the relevant initial report. The main technical challenge for the lawyers will be how to place it onto the statute book in such a way as to affect a wide range of existing laws. However, this type of wide-ranging reform is likely to be necessary for *any* legislation that implements the Electronic Commerce Directive.

1. **Report** of material to be removed

The aggrieved party reports the exact material that is being complained about and the reason that makes it necessary to remove it. The report must identify who is making the complaint so as to enable the ISP to check that the report is genuine. By making a report to an ISP in the UK, the complainant is explicitly submitting to the jurisdiction of the British courts. It would be an offence (equivalent to perjury) to knowingly make an incorrect report. It might be wise to obtain legal advice before issuing a notice, but in straightforward cases this will probably be an unnecessary expense.

The USA legislation requires their OSPs to register a service address for notices. This has considerable merit and will simplify the internal procedures within the industry for dealing with notices. It seems unlikely that any reputable ISP would fail to place themselves on such a register. That said, it would be wise to learn from the American experience and not withhold

all protection from those who fail to register. For example, the registered office could be deemed to be only acceptable address for a company that had not used the registration scheme. It would certainly be desirable to try and prevent the register becoming cluttered by companies and end-users that have no real necessity to be there, but are playing safe.

Until a properly made-out report arrives, the ISP will have no liability for the material it is carrying (except of course material it generated itself). Existing non-judicial methods of getting an ISP to remove material will no longer work, but of course it would still be open for an aggrieved party to go straight to an injunction if this was felt to be a useful.

2. **Removal** of material

The ISP removes the nominated material, in a timely fashion, and reports on this to its author. The identity of the complainant will be given to the author so that they are able to form a fully informed view of their legal position. In removing the material, the ISP is indemnified against both the issuer of the report and the original author of the material, who may or may not have a contract with the ISP.

Some might argue that it is for the author to remove the material, but it is to be expected that the ISP will be able to do this quite rapidly and thus mitigate the damage that is being done. Authors may intentionally refuse to respond quickly and, since "Internet time" moves so much faster than the clock, in some cases this could, in itself, magnify the damage.

In some circumstances it may not be possible to identify the author with any certainty. They may have posted anonymously or have used an email contact address that turns out to be invalid. The ISP will only need to take reasonable steps to identify the author. If they cannot be contacted in a straightforward manner then they will lose the benefit of being notified.

3. **Response** by the author

The author may readily accept that their material should never have appeared – perhaps they posted it to Usenet whilst tired and emotional. The aggrieved party may still take action in the courts, but the likelihood is that in many cases the incident will end here.

However, the author may respond that their material should not have been removed. They may say that it was legal or that a mistake or a misidentification has been made. They can then choose to either fight in the courts or to issue a Replacement Notice to require the ISP to replace the material. Just as with removal notices, false statements would be a serious offence and again the author will need to explicitly submit to the jurisdiction of the UK courts.

The effect of a Replacement Notice will be that the material is returned to public view. If a Court eventually held that material was unlawful, then the act of restoring it would naturally affect the quantum of damages.

We feel that in the great majority of cases, where damage will not be unduly magnified by a slight delay, the author should be given the opportunity, prior to removal, to provide their formal response and thus prevent the material from being removed at all. However, one of the basic premises that the ISP industry is seeking to have established is that the ISP makes no decisions but only provides automatic responses to valid notices. Therefore, if there is to be provision for delay, the situations where this delay would be appropriate would need to be clearly spelled out in legislation.

4. **Replacement** of material

The ISP acts automatically upon any Replacement Notice that they receive. They replace the material and report their action, and its formal basis, to the complainant. Once again, if their action is timely, then the ISP incurs no liability to anyone by doing this.

The procedure ends at this point – a further "remove" notice would not be honoured by the ISP because a "restore" notice already exists. The details should however be passed to the author since this might affect their view of the wisdom of keeping their material up.

The procedure does not necessarily involve the courts at all, but it would be open to either party at any stage to approach the courts and get them involved in the decision as to whether the material should be removed or should stay "up" on the network. Provided the ISP obeys any order of the court, it would not be liable for damages or costs.

The process does not allow an ongoing parade of remove and restore notices from the same complainant, or for the same material. However, there is the possibility that orchestrated campaigns might cause web sites to become unavailable for long periods, through serial issuing of removal notices for slightly different parts of the site. It would be appropriate to allow for formal "restore" notices that cover more than just a single removal, and of course it would be open for a court to order that particular sites have some specified immunity from removal notices whilst a hearing takes place.

Anonymity in the R4 scheme

It is worthwhile to look carefully at the issue of anonymity and how this is dealt with. For entirely practical reasons it has not been made entirely symmetrical between the complainant and the author.

The complainant cannot remain entirely anonymous. If the circumstances are such that the complainant does not wish their contact details to be passed to the author then they will need to arrange to act through an intermediary. However, it is an important part of the protocol that the author is aware who is complaining since that may well colour the response that they make. It is also, from the ISP's point of view, desirable that the author and complainant start communicating directly as soon as possible and not via third parties.

If the author wishes to remain anonymous then they should be able to do so. It should not be possible to determine the identity of an author by the legal device of issuing a spurious notice. The procedures must always encourage the opening of a dialogue between the parties, but they should not lift the veil of anonymity without a proper judicial process that can properly weigh the issues that may be involved.

Conclusion

Mr Justice Morland's judgment of March 1999 confirmed that the Defamation Act applies to material posted on the Internet – which should have surprised no one. However, "notice and take down" is putting burdens onto UK ISPs that foreign competitors do not have. This burden has been increasing rapidly and the publicity surrounding the settlement of the *Godfrey* case is making things considerably worse.

This paper has proposed two ways forward from this position. One is to simply give ISPs blanket immunity so that they need do nothing more than act upon the instructions of a Court.

An alternative would be the "R4" approach, which can be seen "here, now, working" in the USA's Digital Millennium Copyright Act.

There are doubtless other processes and procedures that could be devised. However, it is essential that these procedures become enshrined in legislation – for otherwise the ISP must always assume that existing laws could be invoked at any time.

The key legal supports that are needed within such legislation are:

the ISPs are not liable if they follow the process

and malicious or negligent claimants can be penalised by the courts.

To finally sum up:

When considering what is to be done about contentious content on the Internet, the ISPs should be relegated to an implementation role and their decision-making role should be entirely removed. The public policy result will be that the law will be applied on the Internet without having to co-opt the ISPs as "Judge and Jury".