

---

**Implementing Directive 2001/29/EC:  
Comments on the proposed amendments to the  
Copyright Designs and Patents Act 1988.**

Produced by Paul Mobbs  
on behalf of GreenNet,  
33 Islington High Street,  
London N1 9LH  
tel. 0845 0554011

October 2002.

## Table of Contents

Introduction.....	3
1. Implementation and the Regulatory Impact Assessment.....	4
2. Article 5(1) and Internet service providers.....	6
3. Internet service providers and 'notice to take down'.....	8
4. Balancing criminal liability with a procedure for false or malicious claims.....	10
5. Changes to fair dealing exemptions.....	11
5.A. Use of material for journalistic review.....	11
5.B. The use of recordings by non-profit making organisations.....	12
5.C. Free public showing of a broadcast programmes.....	13
5.D. Exemptions for private study.....	13
6. Digital rights management, data protection and privacy.....	14

## Introduction

This response to the Patent Office/DTI consultation<sup>1</sup> on implementing EC Directive 2001/29 this report has been produced on behalf of GreenNet. GreenNet<sup>2</sup> is an Internet service provider that specialises in providing Internet services to non-governmental organisations and the public in the UK. GreenNet itself is also a member of the Association for Progressive Communications<sup>3</sup>, a global network of service providers working with civil society groups.

Intellectual property rights are one of the growing barriers to online networking. What GreenNet seeks is a balance between the public's interests in the use of information, and the economic interests of rights holders. This is because in an increasingly 'wired' society, restrictions on the use of digital information could restrict, through the economic monopoly of intellectual property rights, the civil and political rights of society as a whole – to a degree never before possible.

GreenNet's interest in the proposed changes to the Copyright, Designs and Patents Act are wider than just those issues that relate to GreenNet's role as an Internet service provider. GreenNet actively campaigns on behalf of its members, to protect their rights to network electronically and to use information technology as part of their own personal or social activities. For these reason our response is not limited to those sections that affect only Internet service providers.

The areas that we are particularly concerned about are:

1. Implementation and the regulatory impact assessment.
2. Article 5(1) and its application to Internet service providers.
3. Internet service providers and 'notice to take down' (*Article 8.3*).
4. Balancing criminal liability with a procedure for false or malicious claims (*Article 8*).
5. Changes to fair dealing exemptions (*Article 5, excepting 5.1*), dealing with –
  - A. Use of material for journalistic review – amending section 30 of the Act;
  - B. Use of recordings by non-profit making organisations – amending section 67 of the Act;
  - C. Free public showing of broadcast programmes – amending section 72 of the Act;
  - D. Exemptions for private study – amending section 29 of the Act.
6. Digital rights management, data protection and privacy (*Article 7*).

These objections are outlined in separate sections below. Substantive comments are displayed in **bold**.

---

1 *EC Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society Consultation Paper on Implementation of the Directive in the United Kingdom*, The Patent Office/Department of Trade and Industry, 7 August 2002

2 See <http://www.gn.apc.org/>

3 See <http://www.apc.org/>

## 1. Implementation and the Regulatory Impact Assessment

Comments were requested on the implementation of the Directive under the European Communities Act, and on the content of the Regulatory Impact Assessment (a point raised in page 3 of the consultation document).

We question whether implementation of the Directive is possible under the European Communities Act. In our view this Directive creates wide-ranging changes to the way that copyright operates. More significantly, the proposals for implementing digital rights management have impacts outside of intellectual property issues – such as data protection and computer security – and merit deeper scrutiny than is possible via the statutory instrument process.

The proposed amendments make a complex and already heavily amended text harder to understand. Given that it is not possible to properly implement the Directive under the restrictions imposed by the European Communities Act, and because the definitions in the Act are already under challenge from other legal reforms (such as the draft Communications Bill<sup>4</sup>), we have to question whether it is wise to further amend this legislation when it is overdue for consolidation.

Later, in relation to Article 7, we discuss the problems created by 'digital rights management' (DRM). As noted in paragraph 57 of the Directive's recital, data recorded as part of DRM must be processed in accordance with the rules on data protection (in the UK, the Data Protection Act 1998). There is no clear means under the Data Protection Act for managing data submitted via electronic networks. Therefore, unless we amend the Data Protection Act, is implementation viable?

**Clarifying the data protection aspects of DRM would require amendments to the Data Protection Act, as well as significant amendment to the Copyright, Designs and Patents Act. These matters also raise significant public policy issues, such as data protection and the use of monopoly economic rights such as copyright, that cannot be publicly addressed via implementation as a statutory instrument. We therefore believe that these issues should be brought before Parliament as a formal revision of the Copyright, Designs and Patent Act.**

In relation to the Regulatory Impact Assessment, in our view the social impacts of changes to fair dealing rules have not been properly quantified in terms of the impacts upon the public, and in particular local community organisations – in particular the changes to exemptions of public performances under sections 67 and 72 of the Act. These uses of copyright work are, by their nature, unregulated and difficult to quantify. But from anecdotal reports, these changes could affect many types of social activity from fund-raising dances for community organisations to provision of a TV in local drop-in centres working with ethnic minorities, women and young people.

**The RIA should therefore seek to provide a more realistic estimate of the impacts on community**

---

4 *Draft Communications Bill*, Department of Culture, Media and Sport/Department of Trade and Industry 2002.

**activities of the changes to fair dealing rules, based upon more detailed research of the extent of unregulated use for community purposes.**

## 2. Article 5(1) and Internet service providers

For some time Internet service providers have sought exemptions from the laws relating to intellectual property and defamation. This is because the automated nature of information systems makes it almost impossible to police all traffic for violations of the law. Such an exemption has been provided in the Directive, but it is restrictive, and in our view it is of little benefit.

Article 5(1) seeks to make the incidental reproduction of a copyright work, necessary as part of the operation of information transmission or lawful use, exempt from the 'reproduction right' under Article 2 of the Directive. The purpose of this exemption is to rectify the long-standing dispute as to whether the transmission of information through an electronic communications system infringes copyright, or whether copyright is implied through the availability of that material online. In fact, the gain from this exemption is illusory for the Internet service provider.

There are two practical aspects to the operation of an Internet service provider:

- 'Information carrier' – the automated relay of information, such as email or network traffic;
- 'Information distributor' – the storage of information for retrieval on demand, such as web sites or other stored files.

The first of these is covered by Article 5(1) – but in any case such an exemption is largely irrelevant. For an infringement of copyright on the relay of information the service provider would have to have prior knowledge that the relay was being used to distribute infringing works. Article 5(1) provides an exemption in this case. But if information were not relayed, but just sent to a service provider's system, that in itself would not be an infringement. This is because it would be the originator of the communication who had made the reproduction of the work, not the service provider.

More significant is the fact that Article 5(1) only relates to the 'reproduction right' under Article 2 – it does not provide an exemption to the 'communication right' under Article 3:

*"Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available 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."*

Therefore, any data that is stored on a system for reproduction on demand – which would include web sites, Usenet newsgroups, stored files accessed via FTP, or information stored internally within an organisation and made available over a local network – could violate the communication right if the transmission of that information was not in accordance with the license of the rights holder.

This incongruity also leads to anomalies in the application of the law. For example, if an email is transmitted via a system containing infringing content then that would be exempted under Article 5(1). But if the email – for example via an email list – were archived and made available as a file for

download, then that would breach the 'communication right' under Article 3.

**In our view Article 5(1) is not a valid exemption. It is a valid exemption for 'connectivity providers' – the network and telecommunications connectivity providers who merely pass data from A to B. But it is not a valid exemption for Internet service providers. This is because their role is not primarily that of an 'information carrier', but as an 'information distributor'. Whilst we welcome of the introduction of Article 5(1), it does not address the particular problems that ISPs face in relation to the liabilities arising from copyright infringement (an issue outlined further in section 3 below).**

### 3. Internet service providers and 'notice to take down'

The previous section outlined our observations in relation to Article 5(1). A separate issue is that, in any case, the exemption under Article 5(1) is not available in all circumstances. The Directive also provides that, even where the Internet service provider has not infringed the rights of any person, or where use of material is subject to an exemption under Article 5, they may still be subject to legal action.

The Patent Office did not see it necessary to implement Article 8(3) on the right to injunct 'intermediaries' – as they consider that this power already exists under UK law. But the fact that Article 8(3), and paragraph 59 of the Directive's recital that outlines its use, have not been implemented does not mean that the application of injunctions in the UK is not affected by the Directive.

The Directive creates a legal remedy for rights holders to seek an injunction against an 'intermediary', such as an information service provider, even where no offence has been made by that intermediary. This right also applies even when the infringing activity the rights holder alleges is exempted under Article 5 (see paragraph 59 of the recital).

If the UK courts were not to grant an injunction against an intermediary, on the grounds that the intermediary had not committed an offence, or that the use of the copyright information was in accordance with an exemption under Article 5, the rights holder could then claim 'direct effect' of the Directive against the court. This is because the Directive grants a legal right to the rights holder from the state, and therefore the 'vertical applicability' test within 'direct effect' is satisfied.

Irrespective of whether the UK courts grant an injunction under the existing law, or whether a test case is brought under the terms of the Directive to clarify the law in the absence of interpretation, we still have the same result. Internet service providers can be legally challenged when they have not committed any offence. This process is then, in all but name, a 'notice to take down' process similar to that under the USA's *Digital Millennium Copyright Act* (DMCA). But unlike the DMCA, the process has no appeals procedure, unless the individual involved has the means to bring a counter-claim in court.

In practise, what this injunctive 'notice to take down' process seeks to do is change the role of Internet service providers. From that of 'information carrier' or 'information provider', to that of a 'content provider' – a carrier who is liable for all the content they provide. This is wholly unacceptable for two reasons:

- The open nature of networked systems means that it is not physically possible for service providers to monitor all the information flowing through their systems. To do so would create such high overheads as to make online services prohibitively high for a large section of the population.
- The potential threat of an injunction, and the legal costs that creates, may lead to abuse of this process through the ability to intimidate service providers. Potentially rights holders would only have to give notice of action in order to get information removed from online systems even though there is no clear evidence of copyright infringement. We must question whether

implementing such as system so easily open to abuse would infringe the public's human rights of expression.

Therefore, the Directive creates a means whereby an individual's service provider may be intimidated into removing their content. But there is no process, unless the individual has the money to bring an action for damages in court, to lift an injunction and get their content restored. In this sense it is far worse than the USA's DMCA because there is no formal appeals procedure for those affected by the notice, and with no legal penalties for false or malicious claims being made by rights holders.

**In our view the use of injunctions against intermediaries is a form of legally-enabled censorship. This is because the intermediary cannot possibly defend against the potentially numerous claims made against them each year. Practicality dictates that they would have to act in advance of an injunction, and therefore the claims of the rights holder will not be legally tested. In our view it is not correct to leave this process open to interpretation by the courts – there needs to be a sure and certain process to allow Internet service providers to operate. Simply deciding not to implement Article 8(3) because something similar already exists is not a sensible approach – we need a process.**

To remedy this problem in the interpretation of the Directive we see two options:

- **Create a formal 'notice to take-down' procedure, with an appropriate appeals process given to the intermediary and the individual affected, that satisfies the process created under Article 8(3) of the Directive. In our view this is still not satisfactory because it loads regulatory burden onto Internet service providers even when they have no fault in the matter. It also is open to abuse because the legal burden still falls on the intermediary rather than the individual responsible for posting allegedly infringing information.**
- **Keep the injunctive procedure, but limit the extent of the effect injunction to the removal of the infringing material, or disclosing the identity of the person posting that material provided the intermediary believes there to be a valid claim by the rights holder. This is a more appropriate option because it limits the liability of the service provider to offer up an identity, or remove the content, should they believe the claim to be valid. It would also dissuade frivolous claims of rights infringement because the rights holder will, in the end, have to pursue the individual posting the material, and that individual will be in a far better position to provide information on whether the information does infringe copyright or not.**

Of these two options, we do not support the (first) formal notice procedure, but instead would support the (second) restricted injunction or notice scheme. Such a system would keep the regulatory burden with those who actually post infringing content.

#### **4. Balancing criminal liability with a procedure for false or malicious claims**

It is proposed to make the primary infringement of copyright a criminal offence. Providing that the current procedure ensures the 'mens rea' test there is nothing particularly wrong with this. The problem arises where false or malicious claims of copyright infringement are made. For some organisations, such as charities, companies, or for individuals who are members of professional bodies, claims of criminal liability can have serious consequences. We must provide a counter-balance to the upgrading of copyright infringement from a civil to a criminal offence by developing a process to address false claims.

Under other parts of intellectual property law, such as trademark, repetitious claims of legal action for infringement where no such rights exists can be remedied in law<sup>5</sup>. In effect, an individual gets an order restraining further claims because it is the opinion of the court there is no case to be heard. However, no such procedure exists for unfounded claims of copyright.

**In our view, if copyright infringement is to be made into a criminal offence then there should be some procedure to guard against repetitious claims of infringement, as already exist under other aspects of intellectual property law.**

---

5 Section 21 of the Trademark Act 1994, '*remedy for groundless threats of infringement proceedings*'

## 5. Changes to fair dealing exemptions

**We oppose any further diminution of fair dealing rights. This is because the development of digital encoding systems actually provides rights holders with far more power to control use than was available with analogue systems.**

Contrary to the view expressed in paragraph 38 of the recital, digital systems do not necessarily lead to an increase in copying. For example, the copying of CDs on home computers is enabled by the fact that the standard audio CD is not a purely digital media – it bridges the gap between digital and audio systems and does not exploit any of the encoding options possible with fully-digital media reproduction systems.

The next generation of digital systems, currently being developed, will encode data to prevent copying. Recent legal cases in the US over the control of encoding and decoding systems, such as the CSS system for encoding digital video disks, show that effective control over digital information systems works not only at the level of the user, but at the level of those creating systems to reproduce these new digital formats. Users are prevented from copying because license-free systems for use or reproduction of digital media will not come onto the market. Also, the proposed next generation of computer systems – for example Microsoft's proposed 'Palladium' system – will be entirely 'locked-up' to prevent copyright infringement. The copying of any file or data device that has the appropriate copy protection permissions set will be blocked by the operating system.

Any person who does not consider that the next generation of digital information systems, to be introduced over the next five to ten years, will be more secure is not keeping pace with the latest developments in digital technology.

**In our view there must be a balance between the potentially restrictive conditions under which information will be controlled under digital systems, and the rights of the public to the use copies of works that they have lawfully bought or borrowed as they wish. Therefore we object to the following changes to the fair dealing rules:**

### 5.A. Use of material for journalistic review

**In our view the Patent Office has improperly transposed the Directive in relation to Articles 5(3)(c) and 5(3)(d). These two exemptions have been lumped together by the Patent Office, but are incompatible for this purpose.**

Amendments to section 30 of the Act<sup>6</sup> creates fair dealing in relation to 'criticism, review and news reporting'. Currently this right extends to all works. But the new amendment restricts this right to only

---

<sup>6</sup> See Annex A, part 4.2 of the consultation document.

works that have 'been made available to the public'. This term of 'available to the public' is outlined in a new section 30(1A). This says that a work is made available to the public if the works owner makes it available to any member of the public – but contains a caveat that if the supply of the work is unauthorised then it has not been made available.

The impact of the revised section 30 will be that any investigative journalist or member of a campaign group who quotes or uses a private, internal or other such restricted document produced by an organisation could be sued for copyright infringement. This amendment has serious implications for the democratic process as copyright could be used as a threat to prevent disclosure of information by the media or campaign groups.

**The amended section 30 does not accord to the Directive. The amendments proposed by the Patent Office implement Article 5(3)(d) – the critical review of works, but they misrepresent the Article 5(3)(c) which relates to the use of material for news and current affairs. Article 5(3)(c) contains no limitation on material that has 'been made available to the public'. The interpretation of paragraph (3)(c) must be separated from paragraph (3)(d), otherwise the new law will seriously affect journalistic freedom.**

## **5.B. The use of recordings by non-profit making organisations**

Currently, under section 67 of the Act, non-profit organisations, clubs or societies can play sound recordings at their events. The condition on such use is that any charge for access to the event only benefits the work of the organisation itself, and that the purposes of the organisation are to advance religion, education or social welfare.

Under the amended section 67 the organisation must show that<sup>7</sup>:

*"that any charge for admission to an event or a place at which or where the recording is to be heard does not go beyond what is necessary to cover the cost to the organisation of holding that event or the operating costs of the organisation in relation to that place."*

In our view this is not a reasonable or achievable condition. The costs of organising community events are not fixed. Setting a gate price that reflects costs, without a shortfall or excess, is not possible. More importantly, to what extent does this condition govern other fund-raising events that take place at such events? Would it affect voluntary contributions given during the event itself?

Most events that use pre-recorded music whilst charging entry for admission benefit local community activities – such as tea dances, community discos, self-supporting youth clubs, and similar community-based activities. Unless the Patent Office can demonstrate that 'significant harm' is being caused to the recording industries by such events, we would argue there is no cause to change the existing law. More

---

<sup>7</sup> See Annex A, part 4.8 of the consultation document.

than that, to change the existing law would cause damage to make local voluntary community activities across the UK.

**In our view there is a balance between the benefits that this currently exempt use creates and the very low level of lost rights revenue to the recording industries. We see no evidence to support the amendment of this exemption, and request that it is withdrawn.**

### **5.C. Free public showing of a broadcast programmes**

It has been proposed to amend section 72 of the Act<sup>8</sup>, which permits the viewing of a broadcast programme by members of the public who have not paid admittance to a place to see it. But the Annex provide no suggested form for these amendments.

**In our view section 72 should not prohibit the free public showing of broadcast services for non-profit making purposes. There are many community activities, such as youth clubs, drop-in centres and self-supporting day centres for the elderly where the incidental provision of a TV broadcast facilitates other activities. As with our objection on the amendment to section 67 above, any amendment to section 72 should not jeopardise the social benefits this exemption currently brings to the community.**

### **5.D. Exemptions for private study**

In relation section 29 of the Act, on private use and research<sup>9</sup>, the requirement for 'acknowledging the source' of information is removed, and instead 'sufficient acknowledgement' must be given. The term 'sufficient acknowledgement' is defined in section 178 of the Act. However, it is a terse description, and often those referencing their work will actually provide a far far more detailed annotation. All the definition in section 178 requires is a title and the name of the author – it requires nothing regarding the publication date, volume or issue of the periodical it may appear in, or the publisher of the text.

**In our view the requirement for 'sufficient acknowledgement' does not work well because, unless a person is well versed in the Act, it is not that clear what the term means. 'Acknowledging the source' would be a far better terms since it is one which those writing referenced materials are more likely to understand. Using this term is also likely to elucidate a more detailed response than one which merely requires a title and name.**

---

8 See the 'summary' section, page 11 of the consultation document.

9 See Annex A, part 4.1 of the consultation document.

## 6. Digital rights management, data protection and privacy

Article 7 of the Directive provides a legal framework for the operation of 'digital rights management'. However, it fails to distinguish between the different systems that exist for digital rights management: 'passive' digital watermarking, 'active' tracking, and 'activation' control.

Digital watermarking – where data is encoded invisibly within the digital information – is simple to enforce as a 'passive' process. If you have a file where the data is missing or corrupted then that person either received or altered the digital information contained within the file.

'Active' tracking and 'activation' control collect and transact data to the computer systems of the copyright holder – forwarding this information via an Internet or other network connection. Illegitimate use of a copyright work in this case will be flagged-up automatically by the rights holder's computer system. In the case of tracking it will mark record for further investigation, but in the case of activation the right holders computer systems can refuse authentication and the program or digital information will not work or be displayed.

All these systems are in use today. Article 7 of the Directive does not distinguish between them. However, there is a very important different between the active and passive systems. Passive rights management systems require the rights holder to police online systems looking for infringing data. However, active systems, because they transact data across networks, create traffic data. In turn they create the potential for the disclosure of personal or potentially sensitive personal information about the user of the controlled work.

This potential for information disclosure is acknowledged within paragraph 57 of the Directive's recital:

*Any such rights-management information systems referred to above may, depending on their design, at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour. These technical means, in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.*

However, there are no controls proposed within the amendments to the Copyright Act to specify the way in which these controls will be applied. There are two general concerns:

Firstly, to what extent can the user ascend to and control the data disclosed from their computer system. This involves not just issues of privacy, but also of computer and information security (see discussion in relation to 'firewalls' below). If the user is unable to control or ascend to the level of information disclosure we question whether these proposals meet the terms of the First Data Protection Principle<sup>10</sup>. Secondly, precisely what controls will be applied to the transaction of data? The Seventh Principles

---

<sup>10</sup> See Part 1, Schedule 1 of the Data Protection Act 1998 for a list of the Data Protection Principles.

requires that:

*"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Any data that a computer collects and forwards to the rights owner via a network could be used to identify an individual's personal preferences, hours of work, geographical movements, and other information that could assist a highly invasive profile of your personal habits. But with access to information about an individual's computer, such as the unique identifying key to the controlled data you possess, others could also forge or 'spoof' your identity in order to provide illicit access to information packages. Access to such information is likely, as computing becomes more mobile, to get easier, so making the security of such information more important.

**It is not specifically defined within the Data Protection Act 1998 as to whether the responsibility for the data processed belongs to the data controller (e.g., the rights holder), or the data processor (e.g., those running the information systems of the data controller), when that data is not resident on their computer systems or 'relevant filing system'. Does the responsibility of the data controller extend across networks to the computer of the data subject? As some of the data processing applied to digital rights management data must be carried out on the data subject's computer, does the current extent of the Data Protection Act 1998 extend far enough to meet the requirements for data protection on the Copyright Directive in paragraph 57 of the recital?**

Another issue is the extent to which data collection may give rise to something more than 'personal data'. If digital rights management only involves authenticating the user's digital identity then only 'personal data' will be involved. However if more detailed information, such as lists of electronic texts read, or database queries submitted, is sent to the rights holder then that could, over time, lead to the rights holder amassing information about that individual's personal preferences. This shifts the data collection from 'personal data', to 'sensitive data'.

**It is not clear within the current definitions within the Data Protection Act would allow the collection of data on a single individual to escalate the classification of that data from 'personal' to 'sensitive'. It is primarily dependent upon the uses to which that data is put. But if digital rights management involves anything more than just authenticating use of the data product on the user's computer, then consideration must be given to the potential impacts of how the collected data will be managed and used – which requires clarification within regulations covering the collection of data as part of digital rights management.**

Digital rights management also has implications for computer security. Any transaction of information via a network brings with it the possibility for a vulnerability to be exploited by system crackers. Therefore, if each software manufacturer used its own system of active digital rights management, a variety of security vulnerabilities could be introduced into a computer system.

For those who wish to improve the security of their network-connected system there is a simple solution – a 'two way' firewall on their network connection. This filters outgoing traffic as well as incoming traffic to prevent unauthorised access. This is not standard on 'insecure' operating systems like Microsoft Windows, which only filters data on the way in, and usually has to be installed by the user. However, two-way firewalls will also intercept and filter and digital rights management communications from the user's system to the system of the rights owner – unless configured not to. This creates two implications:

Firstly, the problem with using a two-way firewall to restrict 'activation' traffic is that the applications reading copyright works may not allow you to block such transmissions – if you do they will fail to operate.

Secondly, and more significantly, if a two-way firewall blocks digital rights management traffic could that person be accused of seeking to evade or alter rights management information under the new section 296ZE proposed by the Patent Office? They would have to prove, in all cases, that the firewall was only for security purposes. But more significantly, the operation of the two-way firewall could in itself lead to the investigation of computer users who innocently use a two-way firewall as an additional security measure.

**In giving a legal basis to digital rights management the Patent Office must also consider whether computer security will be imperilled by these systems. Also, they must ensure that those who protect their systems using technological means do not have that protection diminished via the operation of digital rights management. If digital rights management becomes widespread in coming years, and there is no one centralised system of traffic management for these systems, these new proposals could magnify the possibilities for security vulnerabilities in computer systems, leaving them open to abuse or potentially damaging intrusions.**