

# Law and online order

Government proposals to get everyone online are all well and good but, apart from well-publicised credit card security issues, setting up a website opens up businesses to legal issues similar to those regulating publishing. Jason Whittaker explains more

Until recently, the development of the internet was largely unregulated. Outside its obvious businesses applications, surfing was initially viewed as a geek's pastime. Furthermore, throughout the 80s governments across Europe and the US indicated that they wanted to interfere less in the ways in which companies were run, cutting through the bureaucratic red tape.

This freedom meant the internet developed as a medium to which anyone with a computer and a modem could contribute. The web became established as a free for all – the place where anything goes. For its supporters, this was the triumph of democratic liberalism; for its detractors, the internet encouraged chaos and criminality.

The increased popularity of e-commerce during the 90s raised new concerns. How would businesses be able to guarantee delivery of goods, particularly if they came from another country? How would producers ensure rights over their goods, particularly if these involved intellectual property rights? In what way would firms be able to protect their good name in the case of defamation?

Here, we will look at some of the ways legislation has attempted to keep up with developments on the internet. An article such as this cannot take the place of proper legal advice, particularly if you are concerned about libel or infringing intellectual property rights. But we will highlight some of the most important areas of which you should be aware.

The growth of the internet as an international medium raises its own problems, though tentative consensus is arising on issues such as copyright, defamation, obscenity and privacy.

As Michael Clinch, partner and head of litigation at Picton Howell, points out: "The creation and operation of a website is a legal minefield. Not only do you have to ensure that the site complies with the laws of your home jurisdiction, you also have to be aware that the laws of other countries need to be taken into account."

## Don't copy me

Copyright law covers the form the material takes, rather than the underlying idea. In general terms, anyone who creates something new is entitled to exercise copyright over it. Other people must not reproduce that work, whether in the form of words, visual images or music, without the prior permission of the copyright holder. But you can rewrite or rework the underlying idea into a new form.

Copyright acts follow one of two conventions: the Berne Convention of 1886, revised in 1971, and the Universal Copyright Convention of 1952, sponsored by Unesco and again revised in 1971. In the UK, infringements of copyright are covered by the 1989 Copyright, Designs and Patents Act (amended in 1995). Protection extends for 70 years after an author's death. In May, the World Intellectual Property Organization's Copyright Treaty will update the Berne Convention with specific protection for works distributed over the internet and in other digital formats.

Works may be cited under a rule known as fair dealing for research, criticism or reviewing and private study. Fair dealing does not apply to all types of copyright (image reproduction, for instance), and

→ Anyone working within the EU must be aware of the requirement to protect data

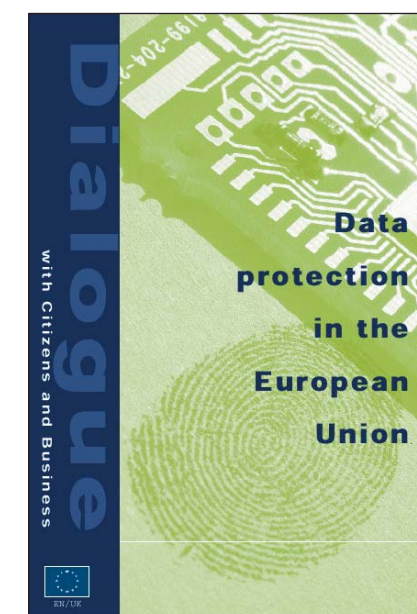
there are restrictions on the amount of material that can be reproduced.

But even the limited amount permissible under fair dealing creates problems when dealing with electronic reproduction. Some copyright holders refuse to allow their work to be stored in electronic format at all because, theoretically, a book or song can be copied across a network an unlimited number of times without deterioration.

## Copyright online

Because of the ease of copying across a network, digital uses are not equivalent to non-digital ones and many copyright holders are pushing governments for tougher regulation. The European Parliament, for example, proposed the Copyright in the Information Society Bill in early 1999, but this introduced its own problems. It caused consternation among the EuroISPA (European Internet Service Providers Association) because it appeared to exclude all copying, including material held in local caches on ISP servers.

The ease with which material can be transferred across the internet, particularly forums such as newsgroups or chatrooms, has led to certain myths and false







assumptions. For example, it is often assumed that if something does not have a copyright notice it is not copyrighted. This is no longer the case – works are copyrighted by default, although this is emphasised by a notice.

As users often do not directly charge for material on the internet, this again makes surfers think it is all right to copy material – most notably in the case of Napster – however, fair use extends only to reviewing, private study and parody.

### Digital rights

The ease with which material can be copied across networks has led to greater focus on digital rights management. One way in which this has proceeded is by extensions to current legislation – for example, through the US DMCA (Digital Millennium Copyright Act), which became law in 1998. In general, the act added to existing legislation by making it a criminal offence to circumvent antipiracy measures or to distribute code-cracking devices or techniques.

The DMCA also limited the liability of internet service providers as transmitters of copyrighted information, as well as the liability of non-profit institutions such as universities when they serve as ISPs.

The new copyright law, while welcomed by content producers, was opposed by many academic institutions and libraries. It has recently been invoked to pursue Dmitry Sklyarov, an employee of Elcomsoft. He must now testify against the Moscow-based company he helped produce software breaking the encryption protecting Adobe's eBook format.

← A shadow of its former self, Napster indicated the trouble ahead for traditional publishers seeking to control copyright

Another way in which web producers have sought to protect management is by using digital rights management software from companies such as Webgenerics and Digimarc. Applications like dotEncrypt (www.dotencrypt.com) enable users to 'wrap' content such as videos, music or documents in an

encrypted format which is then uploaded to Webgenerics' website. To view the content, recipients must agree to a licence either by providing an email address or making a payment.

### Freedom of speech

The internet may provide a revolutionary form of communication, but the freedom and spontaneity it fosters can be a landmine. With the explosion of email, websites, bulletin boards, discussion forums and chatrooms, concern has grown about the web's potential to spread libellous and slanderous statements, disseminate false information and provide a forum for extremist groups.

In the US, the First Amendment to the Constitution guarantees the right of freedom of religion and freedom of expression to all Americans – even those whose opinions may be deemed reprehensible to a

community. What's more, after an attempt to control obscenity and hate speech in 1996 via the CDA (Communications Decency Act), the Supreme Court affirmed that the government could not regulate internet content any more than in traditional areas of expression.

The international nature of the web, however, raises its own problems. In 2000, for example, the Union of Jewish Students and the International League Against Racism and Anti-Semitism filed a suit against Yahoo in the French courts, accusing it of allowing users to buy and sell Nazi memorabilia on its increasingly popular auction sites. Such trade is illegal in France and the company's subsidiary, Yahoo France, had already blocked these sales. But the parent company initially refused either to block the site or to provide warnings and so was threatened with fines of up to £100,000 per day.

The sale of Nazi memorabilia is not illegal in the US as it is in several EU states. Early in 2001, the company agreed to bar the items from auction listings and settled out of court. Ultimately, Yahoo seemed to change its mind because of the negative association that was building up, rather than because of legal pressure. The company issued a statement that it would refuse items 'associated with groups which promote or glorify hatred and violence' – a move that included groups such as the Ku Klux Klan.

### Watch what you say

While hate speech is a problem for society at large, individuals and internet

publishers will more usually encounter difficulties with libel. Although slander and libel are often used interchangeably, slander

→ Buying and selling may not always be easy when it's across international borders, as Yahoo discovered to its cost

is the defamation of a subject by word of mouth, while libel deals with defamation recorded and published to a public audience.

For a charge of libel to be effective, a writer must publish an untruth which is damaging to the subject's reputation and recorded in some permanent form. This can include an email or newsgroup posting. In the UK, a distinction is made between libel and fair comment. To say that a certain actor is overweight may be judged as fair comment, but to say that they cannot act because they are too fat could be considered defamatory.

The best-known recent case of a site getting into hot water because of defamation involved the schoolmate reunion site Friends Reunited. The site owners opted to suspend the message board areas after the National Association of Head Teachers alerted them to abusive comments made about some of its members.

### Libel and slander

Until recently, lawsuits for libel on the internet were relatively rare. However, a number of cases in 2000 and 2001 provided potentially conflicting results across the Atlantic, particularly regarding the status of ISPs in libel cases. This issue has dogged the internet from the early 90s. In 1991's Cubby versus CompuServe case the ISP was treated as a free carrier, much like a phone company, which could not be held responsible for every posting on its servers.

Four years later, in Stratton Oakmont versus Prodigy, the ISP was held responsible. However, this was due to the fact that Prodigy specifically maintained that it monitored the content of its bulletin.

### Demons and defamations

More recent cases in the US have clarified the role of ISPs there, but one (unintended) effect of such rulings was



that they have tended not to monitor content at all to maintain their position as free carriers. The UK government attempted to compensate for this in the 1996 Defamation Act, whereby if the ISP can demonstrate that due care is taken it will not be prosecuted, a so-called 'Section 1' defence.

In the UK, the situation has appeared very different to that in the US. In 1999, a lawsuit was brought against Demon by Dr Laurence Godfrey concerning material posted anonymously to a newsgroup. It was held immaterial that Dr Godfrey and the poster were not Demon customers. Though the case was settled out of court, it is likely that the ISP would have lost. This was not because the material was posted, but because Demon failed to act when the presence of the content on its servers was brought to its attention.

Because of this case, Demon (now owned by Thus, formerly Scottish Telecom) was understandably nervous when Dame Elizabeth Butler-Sloss ruled that the new identities of Jon Venables and Robert Thompson, who were prosecuted for killing James Bulger in 1993, should not be revealed by the UK media. Concerned that it would be taken to court should someone post that information to its servers, Demon appealed and the judge agreed that her original ruling could not apply in its original form to ISPs.

Nonetheless, writers and critics are not immune to laws covering defamation, libel and contempt. Simply because you publish a website without making a profit does not mean that you may not be taken to court. In many cases, web publishing can follow straightforward defamation rules for print and other media, but where a bulletin board, for example, is included on a



## Tips for web publishers

- 1. Careful copying** Even if a piece of published material is not listed as copyrighted it does not mean you have the right to copy it. All material is copyrighted unless the producer has explicitly said otherwise.
- 2. Material limits** Fair dealing is restricted to a limited amount of material (typically 400 words or less) and can only be used for reviewing, criticism, research or private study.
- 3. Foreign rights** If your website is used by members of another country, you need to be fully aware of their local laws. Less importantly, if overseas business contacts are important to your company, having a multicultural site will create the right impression.
- 4. Libel** Remember that you can be prosecuted for libel regardless of whether it appears in a newspaper or on a website's newsgroup.
- 5. The law is right** Under UK legislation, 'publication' includes the transmission of electronic material. If your website contains material that is illegal under British law, simply transferring it to a server located in another country is unlikely to provide sufficient defence.
- 6. Traffic calming** Under the Regulation of Investigatory Powers Act, owners of networks have certain rights (as do other officials) to monitor online traffic. The act also specifies terms and conditions under which such monitoring is permissible.
- 7. One union** Ensure your website complies with EU regulations on data protection at [www.europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf](http://www.europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf).



website, it is the producer's responsibility to manage this as much as possible. This means that postings should be monitored and, more importantly, a complaint-handling procedure should be in place to suspend any postings that may give rise to libel.

### Let's talk about sex

Defining whether or not adult material is obscene has often been problematic. In the US, such definitions for most material rely on whether it is considered obscene by the community at large. In the UK, the 1959 OPA (Obscene Publications Act) is frequently invoked along with the 1990 Computer Misuse Act. A particular problem raised by the internet is the ease with which such material can be accessed from servers in countries where it is not illegal.

However, it is impossible to treat the internet as a completely deregulated zone with regard to sexual matters. In the US, many voters were concerned about their children finding pornography on the web while, in 1995, the Justice Department arrested a number of people as part of an investigation into paedophiles on AOL.

Such activities, combined with fear over what children could be accessing, led to the CDA (Communications Decency Act) on 1 February 1996, which prohibited 'indecent' and 'patently offensive' language on the internet. However, the CDA was judged unconstitutional and suspended soon after. In the UK, the case of Regina versus Graham Waddon (1999) established some of the ground rules for what constitutes obscene publications on the web.

← Demon was one of the first companies to suffer as a result of a libel action taken against an ISP

Under the OPA, it is illegal to publish obscene material with a view to commercial gain – punishment consists of up to three years imprisonment, an unlimited fine or both. The fact that a large amount of pornography on the web is free makes it difficult to apply

the OPA, but Mr Waddon was charging visitors to view his material. His defence was that these files were housed on a server in another country. However, following an amendment in the 1994 Criminal Justice and Public Order Act, publication includes transmission of material to a server, meaning that a person could be found guilty of breaking the law in the UK even if the ISP is in a different country.

### Think about protection

One thing that all internet managers and producers should be aware of is the 1998 Data Protection Act, which came into effect in October 2001. According to this, data transferred outside the European Union from an EU source must follow the same guidelines as European-based firms. The Information Commission has indicated that it intends to visit websites and could take legal action against sites that do not comply with the law.

A report for Consumers International found that European websites were often terrible offenders when it came to protecting data. According to CI's Anne Fielder, "too many companies collect a lot of unnecessary, very personal information". Under the Act, users are not only allowed access to most commercial information held on them, but they can also refuse to give out irrelevant data.

→ The DTI's website contains plenty of useful information on UK regulation

### Changes ahead...

Concern about potential breaches of privacy by surveillance has, however, been overtaken by events on 11 September 01. Following the destruction of the World Trade Center and the attack on the Pentagon, governments in both the US and Europe seem to be keen on introducing more powers of enforcement for intercepting communications.

The so-called USA Act was passed through congress by 96 votes to one in early October last year. This provides police with a range of new powers, including the ability to conduct secret searches at the discretion of the president. In the UK, new legislation will consist of extending the controversial Ripa (Regulation of Investigatory Powers Act), while the Council of Europe is rushing through an international treaty based on the Convention of Cybercrime in the wake of the terrorist attacks.

The Council is keen to close loops in online communications that could be used by terrorists, but the international treaty will cover infringements of copyright, child pornography, violations of network security and computer-related fraud.

The events of 11 September will almost certainly change much of the rhetoric that has informed recent debates about government intrusion into privacy. If this is, as some commentators have remarked, the lasting legacy of the terrorist attacks, then many freedoms of the internet that have been taken for granted in the past few years will almost certainly come under greater scrutiny. ■

