The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0022-0418.htm

Received 25 June 2008
Revised 8 July 2008
Accepted 9 July 2008

PROGRESS IN DOCUMENTATION

Legal issues for information professionals IX

An overview of recent developments in the law, in relation to the internet

Charles Oppenheim
Department of Information Science, Loughborough University, Loughborough, UK

Abstract

Purpose – This paper aims to provide an update to the last major review by Burrull and Oppenheim of legal aspects of information management in relation to the web.

Design/methodology/approach – The paper reports developments in the primary areas of law in relation to the internet since 2004. Topics covered include: copyright, domain names and trademarks, linking, framing, caching and spamdexing (the use of artificial means to enhance one's position in search engines' outputs), patents, censorship, defamation, liability, conflict of laws and jurisdiction and legal deposit.

Findings – The paper shows that legal issues surrounding the internet are likely to become increasingly difficult and that either a new system is needed to resolve disputes, or that a new body of law is needed. It also suggests that information professionals need to contribute more to the ongoing legal debate.

Originality/value – The paper systematically describes legal issues associated with the management of electronic information.

Keywords Information management, Internet, Law

Paper type General review

The topic of legal issues in information management is one that remains of abiding interest to, and high importance for, information scientists and information managers. Information managers constantly encounter legal issues and problems, most notably in the field of copyright, but also in other areas of intellectual property law (such as trade marks and patents), but also in areas of restrictions on freedom of speech and censorship, defamation, encryption of electronic materials, e-commerce applications, etc. Many of these legal issues are also encountered by those in other professions, e.g. spam and internet fraud, but some are either unique to information management or else come up as issues far more often than they would for other citizens. The associated

This is Part IX of an irregular series; the most recent part was: Oppenheim, C. (2005), "Legal issues for information professionals VIII: understanding the recent changes to the law", *Serials*, Vol. 18 No. 3, pp. 186-91.

The author wish to thank Victoria Bird and Victoria Rae for their invaluable assistance in tracking down references for him, and Marigold Cleeve for her assistance in editing this paper. The author also thanks the referees for their helpful comments.

Journal of Documentation
Vol. 64 No. 6, 2008
pp. 938-955
© Emerald Group Publishing Limited
0022-0418
DOI 10.1108/00220410810912460

risks are therefore significant. It is these areas that are focussed on in this paper. Because of the rapidly changing nature of the law and of the situations encountered by information managers, this paper reports developments in the most important such areas of law since the last major review on the topic was written (Burrull and Oppenheim, 2004). In this paper, there is an emphasis on legal issues associated with the management of electronic information. Because it is so much easier to (re)disseminate electronic information world-wide to a large number of people than it is to copy and disseminate (say) printed copies, the legal issues associated with electronic information are that much more fraught with difficulty. Whilst a couple of photocopies of a copyright work might attract mild irritation from the copyright owner, distribution of the same materials on the web to millions will probably result in a lawsuit. Similarly, a defamatory statement made to one person is legally much less serious than one made to hundreds of thousands.

In this paper, consideration is given to recent developments in copyright, domain names, defamation, spamdexing, digital rights management (DRM), legal deposit of non-print materials, patents, censorship, liability for inaccurate or illegal information and conflict of laws. Current trends in the law for each of these topics are assessed.

The rapid growth of the internet, combined with the casual approach to the law taken by many of its most intensive users, have led some to argue that the internet is more akin to the Wild West than to a properly regulated environment. It is sometimes claimed that anything goes on the internet, including copyright infringement, piracy, pornography, slander, distribution of race hate materials, etc. Laws do apply to the internet. However, the law has difficulty in keeping up with developments on the internet. The reasons for this include such difficulties as the rapid changes in technological possibilities, knowing who the perpetrator of some illegal act is, where the perpetrator of an illegal act (or the party to a civil action) is based, and the culture of many internet users, who display an ignorance of, or contempt for, the legal niceties that have been accepted hitherto. A good example of this is the large-scale file sharing of downloaded music, which, despite the advent of iTunes and similar legal services, remains an allegedly serious problem for the music industry. Similarly, the actions of Google with its Google Library project highlight the tensions that can occur when a large corporation decides to test the limits of what the law permits.

This paper's coverage is international, but with an emphasis on the USA and European Union (EU). Because of the rapid changes in technologies, market developments, attitudes, and in the law itself, this paper is focussed on developments since 2003.

Copyright

Copyright law has always involved a tension between copyright owners and users. Publishers rightly want some reward for the investment they have put into creating and disseminating the materials they produce, and wish to control the way materials that they have invested in are exploited. Users want free (both in terms of money spent and in terms of ready access to, and ability to amend and forward) use of materials. Information professionals frequently find themselves in the middle of these tensions. Up until recently, this tension was controlled because technology was controlled. There is only so much photocopying one can do in a day, copy quality problems arise, and photocopying can be relatively expensive. All this changed when electronic information entered the scene. As a result, the tension has increased greatly.

Digital materials raise a number of issues for copyright owners. The first is the ease of copying materials in machine-readable form, or of scanning hard copy. The second is the fact that such copies are typically of high quality. The third is the ease with which people can place machine-readable items on the web, and thereby pass them to potentially millions of individuals. The fourth is that such copying or transmission can be undertaken at little or no cost and is extremely fast. The final issue is the difficulty in policing such actions. As a result, rights holders tend to argue that some copying that was considered acceptable in the paper environment would not be acceptable in the digital environment.

Copyright owners have responded to the digital challenge by adopting one or more of three approaches. The first of these is to lobby for a strengthening of copyright law, combined with a policy in some industries, such as a music industry, of vigorously pursuing infringers through the courts. This approach has been very successful at strengthening the law. The second is to develop so-called technical protection measures (TPM) (also sometimes known as Electronic Copyright Management Systems, Electronic Rights Management Systems, Technical Protection Systems or Digital Rights Management Systems, though, as explained below, strictly the latter term is broader than just devices to prevent access to electronic materials) to prevent copyright abuse, and to have laws in place to make unauthorised bypassing of such technical measures a criminal and/or civil offence. Lessig (1999) has memorably called this "code". The third method is to lock users into licences that control what they may, or may not do with the electronic materials to which they subscribe. Perhaps, surprisingly in view of the ubiquity of such licences, there have been relatively few works advising information managers on how to handle licence negotiations (Giavarra, 2001, Harris, 2002, Durrant, 2006). The British Library (n.d.) has provided an interesting and eye-opening analysis of the types of controls imposed by licensors on it. Despite the cards apparently being mainly held by the rights owners, information managers have not been idle in response to the perceived threats to their ability to fulfil their patrons' needs by these rights-owner moves.

Anti-cartel laws mean that publishers are not allowed to jointly impose uniform licence terms on patrons. However, they do not stop libraries and information units from creating consortia, i.e. unified purchasing organisations. These can and do negotiate with publishers from a position of strength. Consortia licensing deals are becoming increasingly common, especially in the education sector. Consortia are particularly useful because members can learn from each other not to be intimidated by legalese, and to identify what clauses should, or should not be present in a licence.

Finally, there are statements of licensing principles. These are statements issued by groups of information professionals, or their professional bodies, regarding the minimum terms they expect from licences (for example, that users must be permitted to download and print out items), and statements about terms they regard as unacceptable (for example, prices that are far higher than the equivalent print product, or contracts where the supplier reserves the right to increase prices without notice). They strongly advise librarians and information managers not to sign any deal that does not conform to these principles. Bottom line positions and deal-breakers have been identified in some of these statements. In some cases, Model Licences are also available for people to consult (Cox, n.d.; NESLI, n.d.).

The pressure for changes in the law to tilt the balance of rights away from users, in particular by reducing or removing exceptions to copyright, and in favour of owners comes from the major music, software and media corporations. Publishers have not traditionally been in the forefront of this pressure, but are happy to be associated with it. Other than in the USA, the important changes do not take place at a national level, but rather at the international level. In particular, they come through pressure on the World Intellectual Property Organisation, the World Trade Organisation and at the EU level. The content industry's drive towards increasing rights and reducing exceptions to copyright has, not surprisingly, been criticised by the library and information community and by some legal experts, such as Lessig (2004). These changes in the law can be grouped into four areas.

Firstly, there is a trend towards lengthening the term of copyright. In the case of Literary Works, this has been extended in many countries to life plus 70 years. Today there is pressure to increase the lifetime of sound recordings from (typically) 50 years from the date of recording to (typically) 95 years from the date of the recording.

Secondly, there is a trend, led by the EU, but being considered by other countries, to provide special protection for databases, that is to say, collections or compilations of facts, data or other materials. WIPO considered developing a Treaty on database law in 2006, but shelved the idea at the time as it was too controversial. In many countries' laws, the protection for such collections is ambiguous, weak or non-existent. An EU Directive introduced a new right, the so-called "database right" for such collections of data (Davison, 2005; Derclaye, 2008). There have been attempts to introduce similar rights in US legislation, but so far without success. Indeed, all is not plain sailing with the EU database right. A recent review of the right, commissioned by the EU (European Commission, 2005), found little evidence that the new right helped the European database industry. Furthermore, a key European Court case, *British Horseracing Bureau* v *William Hill*, drastically reduced the degree to which the right could be applied to databases.

The third move is to enhance the protection given to materials in a networked electronic environment by developing a new restricted act, namely the act of communicating a copyright work to the public. In other words, putting third party material up on the internet or on an intranet without the permission of the copyright owner becomes infringement.

The final change is to make it illegal to tamper with any copyright information on a copyright work, or to try to by-pass or deactivate any technical fix that prevents people from using copyright material, or which meters their use for the purpose of charging them. All told, the trend is to change the law in favour of rights-owners and away from users. This could lead to increasing polarisation between users and owners, with the librarian/information information manager in the awkward position of trying to encourage respect for laws with which the librarian/information manager may have little sympathy.

One of the major areas of copyright litigation in recent years has been in the field of musical, rather than textual data and relates to file sharing. The music industry understandably argues that file sharing damages the sales (and, by implication, the profits) of its titles. The evidence that file-sharing damages record industry sales is controversial; just because someone downloads music does not mean they would have otherwise purchased it, and indeed, possibly downloading enhances rather than damages sales overall as fans are exposed to new genres or musicians they had not heard of before. One remarkable development in recent years has been the success of the legal file sharing services such as iTunes. Its success has led to a transformation in the business model for the music industry, and, indeed, appears to have reversed the growth of illegal file sharing (Bakker, 2005; Lex, 2006). This is a crucial demonstration of how technical advances can be viewed as an opportunity rather than a threat.

The major problem for the music industry is that there are many different services offering illegal file sharing, and as soon as one is closed down, another appears. It is also extremely bad for PR and marketing efforts to sue one's own best customers.

Another major development in copyright in recent years has been its role in Web 2.0. Major problems arise regarding ownership of, and rights to reproduce, e mail threads, discussion list threads and materials in blogs and wikis. The position is further complicated by the question whether there are implied licences to reproduce materials which are contributed to such Web 2.0 applications, much as there is an implied licence to reproduce a letter written to the editor of a newspaper. Both Gringras and Todd (2008) and the Web2Rights (n.d.) web site provide helpful guidance on these issues, but it must be stressed there is no clear case law as yet regarding these topics.

Digital rights management

In recent years, there has been significant expansion of interest in DRM. DRM at its most basic level is a set of techniques and protocols designed to identify who owns rights to materials and what can or cannot be done with that material. In many people's minds, however, the term is conflated (incorrectly) with TPM, i.e. hardware and software methods that deny access to copyright material unless the user can demonstrate that he or she is permitted access, e.g. by means of an ID and password, or by entering credit card details. Strictly speaking, DRM embraces TPM and a lot of other things, but the two terms are synonymous in the minds of many. There are a several legal issues regarding the use of TPM. The first is the protection afforded to TPM by the DMCA and by the EU Directive on Copyright. Both sets of legislation make it an offence to by-pass or deactivate a TPM (or copyright management information, such as the details of the copyright owner and tracking of usage made of the document). Problems however, arise when the bona fide user is trying to by-pass such a technical protection system in order to enjoy an exception to copyright. Exceptions to copyright are considered to be under considerable threat with the trend towards stronger copyright laws and with the promotion of licences that might sometimes reduce users' rights (Burrell and Coleman, 2005; Guibault, 2002).

The second legal concern is privacy and data protection. TPMs enable the tracking of usage by the individual user. Within the EU, such tracking is lawful, but only if the user has been informed that the tracking is taking place, and has given his/her informed consent to such tracking. It is not clear what would happen if the user refused such consent either at the beginning of a session, or after the event. Although privacy issues have been raised several times, developers of TPMs do not seem to have addressed them fully yet.

The final legal issue raised by TPM is its link with contracts. A TPM gives the copyright owner a very strong bargaining position. It can be argued that a TPM extends copyright owners rights to, e.g. preventing the displaying, printing and making of back up copies of digital materials, which would be lawful in a printed product, and as such is contrary to the public interest (May, 2007; Gillespie, 2007).

Overall, DRM tend to be associated with barriers to access (though they do not have to operate in this way, and can simply be a way of informing users of what can and cannot be done with the materials). Cunningham (2004) provides an interesting philosophical analysis of whether DRM can ever be justified.

In part in response to these issues, two major developments of note have occurred, i.e. Creative Commons and Open Access.

Creative Commons

Creative Commons licences (Creative Commons, n.d.) are used by a wide range of individuals and organisations, and can be viewed as a component of the Open Source software movement, which is not, however, discussed in detail in this paper. Creative Commons licences, aimed at the electronic content market, allow third parties to copy freely materials placed on the internet, as long as certain rules are obeyed. The most important rules are that the creator's identity must be retained. Other rules that can be imposed by the creator is that the material cannot be used for commercial purposes, that it cannot be amended or incorporated into other materials, and that the copy must have the same rules applied to it as the original, i.e. it can be further copied, subject to the same ground rules as already imposed, i.e. it is a so-called "viral licence". By definition, Creative Commons licences are incompatible with TPM systems. The movement originated in the USA under the leadership of Lawrence Lessig, but has spread worldwide with local versions of licences, reflecting local laws and languages, springing up in many major economies. Derivates of Creative Commons licences, such as Science Commons licences for scientific data, are under development. A number of commentators have argued that Creative Commons represents a breakthrough, avoiding the confrontational stance of some copyright owners but avoiding anarchy caused by a total lack of copyright. The popularity of Creative Commons certainly indicates a wish by many to move away from the rigidity of current copyright law and attitudes, and it represents a genuinely hopeful development in the copyright arena. However, as with Open Source (Ciffolilli, 2006), Creative Commons materials might be incorporated into proprietary materials by unscrupulous organisations. Thus, owners of Creative Copyright materials have to remain vigilant that their materials are not being abused. There is a clear overlap of interests between the proponents of Creative Commons and those who support the idea of knowledge as commons (Hess and Ostrom, 2007).

Open Access

Similarly, the development of Open Access (OA) has been rapid in recent years. OA means, in essence, that an electronic version of scholarly material is available free of charge to anyone with the necessary technical equipment to access it. There are two primary routes to OA materials. The first, the so-called "gold route", is OA journals, which are free of charge to the user. Some are run at no cost through volunteer effort, some receive sponsorship from commercial organisations or charities, and some receive money from authors in the form of author submission fees or paper acceptance fees. Combinations of these funding sources are of course, possible. The Directory of Open Access Journals (n.d.) provides a listing of current journals, but it must be said some of the entries are suspect as they represent journals that appear to be moribund. Some journals published by, e.g. Springer, Blackwells and Oxford University Press, offer authors the choice of no charge for submission but the paper is only available to subscribers, or the author pays a fee and the paper is open to anyone. There is no reason why OA journals should not have rigorous refereeing standards – it is certainly not just a form of vanity publishing.

The second method, the so-called "green route", allows the author to get his or her paper published in a traditional toll-access journal and in addition to place a copy of it (the process is often called self-archiving) in a repository (either a subject-based one, such as ArXiv (n.d.) for physics, or an Institutional repository, associated with a particular organisation, e.g. a University). Many of the most prominent advocates of OA regard the green route as the best route, and regard the gold route as an irrelevance, or as something that is seriously distracting the focus of the OA movement. In recent years, much has been written about the technology, and costs of OA, but it is clear that the biggest single barrier to getting repositories populated is cultural and legal. Cultural barriers involve persuading academics to do it. The legal barriers, i.e. copyright, arise from the fact that too often, scholars assign copyright in their paper to a publisher, and then feel they are not able to (in effect) re-publish the paper in a repository. In practice, most of the major publishers are OA-friendly and do not object to the placing of the item in a repository – albeit often after an embargo period. The well-regarded SHERPA/ROMEO database (SHERPA, n.d.) provides a list of the major scholarly publishers of the world, together with information on their rules regarding self-archiving. A Directory of Open Access Repositories (n.d.) is available. Jacobs (2006) provides a good overview of OA, Jones *et al.* (2006) of Institutional Repositories and Willinsky (2005) provides an excellent explanation of the philosophical principles behind OA.

In addition to Creative Commons and OA, many in the software community continue to support Open Source, and continue to use the internet to disseminate methods of by-passing TPM (Eschenfelder and Desai, 2004).

Legal cases

In recent years, there have been many notable legal cases regarding copyright, but perhaps the most important one has hardly begun. Google plans to digitise a large number of books, both in the USA and the UK, and then will offer a search service so that people can identify books, many of which are out of print, from the use of keywords, and can inspect an extremely small portion of the book online. This has led to an angry reaction, and a number of publishers and author groups have started legal action against Google. Under US law, there is an arguable case that its generous "fair use" provisions make Google's actions legal. The company's legal position in other countries' law is less favourable to it. The primary focus of the complaints is not so much that Google's actions will damage sales (indeed, arguably they will help sales), but rather that copyright gives the owner the right to authorise, or refuse to authorise, copying of the work, yet Google is copying works without seeking permission, i.e. it is a matter of principle that is at stake rather than lost profits.

Conclusions

Copyright continues to be a battleground between copyright owners and users. Developments in technology and the emergence of an internet culture that is frequently and openly antagonistic to the entire concept of copyright mean that problems associated with copyright on the internet are likely to increase rather than decrease in the future. However, there are some optimistic signs of developments, such as Creative Commons and OA, which will help by-pass some of the problems.

Domain names and trade marks

A trademark is a distinctive symbol that identifies through established use particular products or services of a trader to the public. The symbol may consist of a device (in other words, an image, shape or colour), words, or a combination of these. The owner in general enjoys the exclusive right to use the trade mark in connection with the goods or services with which it is associated.

Domain names form parts of e-mail addresses and URLs. Each domain name can only refer to one IP address. Domain names are attractive because they are memorable, and tell a bit about the organisation. There has been an international race to become the owner of convenient or prized domain names. Domain names must be unique worldwide, whereas trade marks need only be unique within a particular class of goods or services and within a particular country. Thus, it is perfectly possible to have several identical trade marks in one country. Duplication of trade marks in different countries is also extremely common. The problems of applying local jurisdictional powers on something as international and nebulous as domain names is summarised by Bainbridge (2003).

Domain name disputes can be broadly classified into a number of headings:

- Two or more *bona fide* organisations quite legitimately claiming, owning or using the same or similar name or brand, sometimes called competing proprietary interests.
- Cybersquatting – taking a valuable name identical to that of a well-known large corporation. This may be followed by a demand for money from the corporation in return for assignment of the domain name to the company.
- Unofficial fan clubs that wish to adopt the name of their hero, team, cult TV programme, etc.
- People who have chosen to use versions of well-known names to spread negative publicity about an organisation.
- Deliberately misleading domain names that lead users into race hate, pornographic or similar sites rather than the one they were expecting to reach. A classic example of this is www.martinlutherking.org/
- Advertising competitor products on search engine results after the user has entered a search for a particular company.
- Spamdexing is the use of methods to ensure the appearance of a particular web page high up in a search engine's output. Some of the methods used are perfectly legal, some are legal but unethical, but the focus in this discussion is the methods that are illegal. These involve the use of trade marks in the meta-tagging or other text associated with web page. This is discussed further elsewhere in this paper, but it is worth noting already that the legal protection of trade marks is limited to particular classes of goods and services and within particular geographic territories, and to get world-wide protection for all goods and services is difficult to achieve and extremely expensive.

Virtually all courts in the world have decided on certain common principles in these cases. These can be summarised as follows:

- the first one to register generally, but not always, wins;
- courts tend to rule against cybersquatters;

- the question of whether the domain name and/or the Registered Trade Mark is actually being used, and how long it has been used for, is very important; and
- the greater the reputation of the Registered Trade Mark, the greater the likelihood of success; but on the other hand, if the domain name comprises generic or common words, it is less likely that the plaintiff will succeed.

It is worth noting that other laws may apply in such cases, e.g. the use of registered company names by an unauthorised third party is illegal in many countries. In addition, a number of countries have passed explicit anti-cybersquatting laws (Walsh *et al.*, 2003).

It is likely that many organisations will encounter a dispute either as litigant or defendant sooner or later. The importance of registering relevant domain names, and of scanning for new names that might compete with your own, cannot be over-emphasised.

Linking, framing, caching and spamdexing

Linking

There are some areas of the law wherein the internet has introduced completely new problem areas, and where existing laws and precedents have had to be stretched to accommodate the new issues. Linking provides a good example. The very fabric of the web depends on linking, yet there can be circumstances where such linking is controversial. It is reasonable to assume that placing material on a web page gives others an implied licence to create links to that page, but does not give an implied licence to copy or disseminate without permission substantial portions of the web page.

There have been many court cases around the world regarding linking, and it is difficult to generalise about the results. Simple linking to another home page by providing a URL or one or two words as the linkable element does not appear to be legally problematic. The problems arise when a substantial portion of the linked document is copied over, or when deep linking is involved. In the case of deep linking, the link is not to the home page but to an internal page of a third party's web site. As a result, users bypass the homepage which might contain advertising, potentially decreasing the owner's revenue, or the homepage might contain a click through to the owner's licence agreement (which might be a Creative Commons licence) or a disclaimer statement by the web site owner. Depending on the specific circumstances and the country in which the court case was heard, such deep linking has sometimes been found to be illegal, and sometimes legal. This is an area where caution is required; it is always best to seek permission if one is proposing to deep link and thinks there is a chance the other web site owner might object (Rowland and Campbell, 2002; Markel, 2002).

In contrast to the uncertainty of linking, framing third party materials is almost always illegal. This is where linked material is placed within a frame that leads readers to believe the material they are reading is within an organisation's web site when in fact it has been drawn from a different organisation's web site.

Another important area of law is spamdexing, which can be defined as the methods used by a web page's creator in order to ensure that his pages appear in as many search outputs as possible, and that the pages are as highly ranked in those search outputs as possible. Spamdexing started with embedding buried text (invisible words, repeated many times) inside the web page. More recently, it has involved putting words like "sex" or "mp3" as tags, irrespective of the actual content of the web pages. There is nothing illegal as such with attempting to exploit search engines' ranking algorithms to ensure one's page appears in the first screenful of search output. The only legal issues arise when the tagging involves the use of words that are a third party's Registered Trade Mark, without permission. In such cases, Courts have shown themselves sympathetic to the Trade Mark owner where the tagging has no bona fide reason to employ the Trade Mark. Spinello (2002) considers some of the ethical and legal issues associated with spamdexing.

Patents

Information managers are most likely to encounter patents when those patents cover software and/or so-called business methods (where software is used to improve or to maintain quality in some process or other). Patent law is stronger than copyright law in the sense that to infringe copyright you must deliberately copy the original material, but to infringe a patent you may well not even be aware of the patent's existence when you make, use, sell or import something whose effect is covered by a patent's claims. To gain a patent, amongst other criteria, the applicant must demonstrate that the invention is new, and that the invention does not fall under one of the areas deemed not to be patentable by the country's Patent Office. A problem has arisen, however, because the US Patent and Trade Mark Office has been granting patents for software and business processes without sufficiently rigorous checks whether the invention is new or not. As a result, there has been a flood of US patents in the software area, which are of dubious legality.

The USA has adopted a more liberal approach than Europe. In contrast, the European Patent Convention declared the exclusion from patentability of software "as such". Although the European Patent Office has taken a broad view of interpretation of this wording, and despite efforts by some corporations to get it to be more generous in granting software patents, its approach has been stricter than the USA.

Patents are also controversial because of the use of so-called "submarine patents", i.e. patents that have been granted but that the owner keeps quiet about until the owner suddenly springs one or more allegations of infringement on unsuspecting individuals or organisations (a recent example was that of Blackboard suing Desire2Learn over the alleged infringement of Blackboard's patent for a virtual learning environment). This practice, not uncommon in the USA and often relating to software or business process patents, has made the need for those who make, use or sell software to ensure they are not infringing all the more important.

Two types of intellectual property, namely copyright and patents can cover software. It can be argued that if software is to be patentable, then it should not be the subject of copyright; in other words, the software industry cannot expect to have it both ways. Having said that, many industries rely on a combination of intellectual property rights for their profits, so why should software not be patented? Plotkin (2003, 2005) discusses the case for and against allowing software to be patented and Tang and Pare (2003) challenge the idea that the software industry needs patents at all. Leith (2007) considers the laws relating to software patents in Europe.

A key problem is the lack of patent examiners who know how to identify software patent applications that are invalid. Once that problem is addressed, the complaints about software patents may go away, though there are some authors (Jaffe and Lerner, 2007) who believe the problem is more fundamental than that.

Censorship

The internet provides great freedom to people to promote their products, services or opinions, but with that freedom comes the risk that objectionable materials will be found on the internet. This includes web sites that promote racial hatred, terrorism, religious hatred, violence and pornography. In addition, in many countries, political web sites that represent opposition views are unacceptable. Of these objectionable materials, pornography has been the one that has been written about most, although some commentators argue that other types of objectionable material are more pernicious.

There is little doubt that pornography is the biggest seller in terms of materials that some find objectionable that is on the internet. Of course, librarians and information managers will also encounter objectionable materials in print and other formats. The problem with objectionable materials on the internet is that local laws and local police actions are bound to fail in a medium that is international and where it is so easy to hide one's true identity as well as where one is hosting materials.

Some governments have taken a rigorous approach to solve the issue. For example, PR China has sought to regulate its own internet industries and has imposed restrictions on how people can access the internet. The recent case of Google agreeing to censor the amount of material available to its Chinese customers is a case in point.

Librarians often find themselves in the forefront of fights against censorship. Traditionally, the librarian's role has been to provide access to such information that patrons require, but clearly financial limitations mean that at all times librarians are making conscious decisions to provide some materials and not others. The ethical issues involved in making such decisions and in particular whether patrons should be protected from exposure to objectionable materials, are difficult to resolve. The CILIP (n.d.) web site provides some guidance. Various codes of ethics exist, but they rarely provide the kind of concrete advice that librarians need to resolve a particular situation. The existence of journals (such as *Journal of Information Ethics*) and of professional associations (or special interest groups of professional associations) directly concerned with ethics, censorship and freedom of information demonstrates the importance and concerns felt by library and information managers when dealing with these issues. A typical example of the types of problem that can be encountered is the use of filtering software. The filters take three forms. The first is screening documents before allowing access. These tools are able to detect forbidden words such as "breast", "sex" and so on. Of course, as with many IR systems, such software does not offer 100 per cent recall or precision. Moreover, the rates of errors of such softwares can be high, blocking for instance the Superbowl XXX or Dick Cheney's web sites. A particularly interesting example of such software is Covenant Eyes (n.d.). This is a service that an individual subscribes to and which then provides a regular report to that individual, or to nominated third parties, of what web pages the individual has visited. It rates these web sites by their objectionable content, and at first glance, the reports appear to be reliable and so this could, perhaps form the basis of an effective filtering service. Although features of this service are the subject of a US patent application (DeHaas, 2007), the algorithm used is secret, and the service does not appear to have been objectively evaluated so far. The second approach relies on third-party organisations to evaluate all content by individual inspections, and to then use simple software to prevent access to particular classes of materials. The final approach is close to self-regulation, whereby systems such as platform for internet content selection are used to rate content by the content creators themselves. These systems, however, suffer from the key disadvantage that they are dependent upon the voluntary agreement of producers to participate, and, for those who do, the accuracy of their coding.

Issues such as pornography put librarians in the front line again. They continue to need to strike a balance between the need for free access to information and society's wish to protect its vulnerable citizens against harmful materials.

Defamation

It is not surprising that increasing amounts of defamatory material can be found on the internet. The defamatory material can be spread through printed publications, images, moving images, sound recordings, newspapers, e-mail, bulletin board postings (and analogous group communications) or via the internet or related sources.

Defamation law attempts to balance the right to protect one's reputation with the right to freedom of speech. Countries vary greatly in the respective weight they give to these two concepts. Whilst some countries, such as the UK, are regarded as plaintiff-friendly, the USA, with its important First Amendment to the Constitution, gives commentators greater freedom to criticise others. There is no sign yet, despite the ubiquity of the internet and the potentially defamatory material contained within it, that different countries' approaches are converging (Collins, 2005). This remains a particularly problematic area for information managers, and they need to ensure that clear guidance is given to their colleagues regarding the legal risks of posting defamatory materials on the internet (or indeed, on an intranet or similar), and also should ensure that their employers have robust notice and take down procedures in place in case of complaint, and that appropriate insurance cover is obtained. They need to bear in mind that the legal action may take place in another country if the defamatory material is available in that other country. In many countries, the employer can be sued for the actions of its employees even if what the employees did was contrary to rules laid down by the employer (so-called "vicarious liability"). This, combined with the ease of making defamatory statements on (say) an electronic informal discussion group means that information managers need to remain vigilant in this important area.

Liability

What is the liability of an information provider (which may be a librarian/information manager, or could be a database provider or an internet service provider) providing inaccurate information and thereby causing a plaintiff financial, physical or other types of damage (Hann, 2003; Joint, 2003)? Similar questions arise for other forms of illegal material passed on, such as pornographic materials. Courts tend to take the view that the information provider is liable if it knew, or had good reason to know that the material was illegal or likely to cause damage. However, that general overview covers a multitude of different situations and possible outcomes and some authors argue that rules regarding liability are not strong enough to protect consumers (Prins, 2003). One cannot always assume that the injured party cannot use professional judgement to query or reject the information on offer. The liability risks increase if charges are made for the supply of information, but the mere fact that a charge was made does not automatically mean the information provider is liable if the recipient should have known better than to rely on the information. Thus, each case has to be treated on its merits. Perhaps, surprisingly, considering how uncertain this whole topic is, very few cases have occurred worldwide where librarians or information managers have found themselves sued or prosecuted for the supply of erroneous or dangerous information.

In the USA, the DMCA has attempted to clarify the law by providing ISPs immunity from liability as long as the ISPs adopted specified "good citizenship" policies. These include the removal of alleged infringing material from the internet and the termination of abusive subscribers. The European Directive on Electronic Commerce is also of relevance. It had the aim of removing inconsistencies in Member States' legislation and case-law concerning the liability of service providers acting as intermediaries, which "prevent the smooth functioning of the internal market". It is unfortunate that major countries' laws are not fully aligned in this important area of law (Rustad and Koenig, 2005; Collins, 2005).

Whilst clearly, some governments have made efforts to exclude the liability of ISPs from many of the illegal activities of their subscribers (Sutter, 2003), the same may not be true for either employers or librarians. Information professionals will need to keep a close eye on what their patrons get up to and should develop robust policies to ensure the level of illegal activity is kept to a minimum.

An interesting issue arises from the question whether one should be monitoring materials passing through a particular web site or from a an e mail address at all. One argument is that by checking such materials, one then is acting as an editor, and if anything illegal is disseminated, then the controller has lost any immunity from liability and can be sued. The suggestion therefore is that it is best for a controller of a system to turn a blind eye to the use made of that system. Other legal experts, however, have claimed that failure to check when one should have guessed something illegal was going on would not provide any immunity.

Conflict of laws and jurisdiction

One of the most problematic areas of internet law is that of jurisdiction, or choice of law (the terms are often used interchangeably). There have been differences in law between countries since countries first codified their laws. In the past, this did not prove to be a major problem, since the law of the country in which the offence or dispute occurred, would always take precedence. Areas outside national jurisdictions, such as the high seas and outer space, developed their own laws or agreed procedures. The particular issues that arise in the internet environment include identifying the defendant, the transient nature of internet evidence and the transportability of site (Kohl, 2007). There are other issues associated with deciding where exactly internet transactions have taken place (Reed, 2004) and the possibility of one's operations to a jurisdiction where the activities to be carried out are legal or are tolerated.

In theory, well-established principles can be used to handle internet disputes or claims of illegality. All that needs to be shown is that the offence is actionable in the local courts, and that either some damage or illegality was done in the country in question, or that the source of the damage or illegality was based in that country (Bigos, 2005). But practical enforcement is a different matter. Criminal and civil jurisdiction are thereby frustrated (Deveci, 2005, 2006). The problem is not just between countries, but can be within a country if it has a federal structure, as in the USA.

A typical problem arises when two jurisdictions take opposing views of the same case. In the well-known example of Yahoo, a French Court found the company guilty of breaking the (French) law regarding the promotion of Nazi memorabilia, but a California Court told Yahoo it could ignore the decision, as it was a US-based company and the company had broken no US law. This case remains as a stand-off, and it is difficult to see how it can be resolved satisfactorily (Saadat, 2005). It represents a clash between the First Amendment to the US Constitution, which allows individuals and organisations to express reprehensible ideas and policies, and the national law of France, which prevents such activities.

Legal deposit

In recent years, a number of countries, including the UK, have adopted laws requiring or enabling the legal deposit of electronic materials published (however that term may be defined) in their country. In addition, the Internet Archive (n.d.) is the best known attempt to capture much of the material on the internet for future generations. Another example is the UK Web Archiving Consortium (Bailey and Thompson, 2006). The latter service is probably, strictly speaking, infringing copyright, but in practice, organisations that own web sites do not appear to object to its activities. Indeed, its heaviest users include copyright and patent lawyers who use it to collect evidence of, e.g. prior art to invalidate a patent application.

Ayre and Muir (2004) and Kavcic-Colic (2003) have reviewed some of the legal issues involved in archiving the web. The fact remains that many countries' laws either prevent (through its copyright legislation) archiving by other than the copyright owner, or fail to implement appropriate legislation to enforce legal deposit of such materials (for example, the UK passed its Act (Legal Deposit Libraries Act, 2003) in 2003, but to date the Act has not been properly implemented for non-print materials). This is a matter that will be of growing concern, not just to those who wish to use such archives today but also for historians of the future. There are, it is true, many legal, technical and economic issues to be overcome in developing legal deposit legislation for non-print materials, not least in deciding where something has been published and enforcing any legal requirement to deposit, but the slow progress throughout the world is a matter of great concern to those involved.

Conclusions

The electronic environment poses a large number of difficult legal issues that information professionals have to face in their daily working lives. The indications are that the issues will become more difficult in the coming years. Although, except in the area of censorship and filtering software (and in the USA, disputes regarding information on patrons' reading and borrowing habits being passed to the FBI in the light of recent terrorist outrages), information professionals have not yet found themselves in the front line of court cases, there is no reason to think this will continue to be the case.

However, there is another, more fundamental question that needs to be addressed. It is often difficult to apply traditional legal concepts to criminal and civil disputes relating to the internet; this, combined with the obvious lack of respect for copyright and other laws shown by internet users, and the development of alternative approaches to traditional legal approaches, such as open source, Creative Commons and a growing interest in usufruct as an alternative to copyright (Porsdam, 2006). Hope (2008), in a study of whether Open Source principles can be applied to biotechnology, presents an in-depth scholarly exploration of the Open Source phenomenon and in particular, examines its characteristics and relationship to both patents and copyright.

There have been arguments that new bodies, based upon the lines of ICANN for domain name dispute resolution, are needed (Von Bernstorff, 2003; King, 2004; Hart and Rolletschek, 2003) or, more radically, that a new body of law is needed. This new body of law would not just apply to information professionals, but also to all who come into contact with the internet. In particular, a law for cyberspace that is distinct from existing law may well have to develop to address some of the problem areas outlined. Arguably, the development of the internet presents an excellent opportunity for the development of a body of international law, which will stand side by side with, e.g. the laws of exploitation of Antarctica, as examples of genuine international agreement on legal principles. So far, alas, there is little evidence of such a radical development.

There remains a surprising lack of systematic research into legal issues undertaken by information professionals. Whilst information professionals have written many articles on legal questions on the internet, they are mainly descriptive of the problems. At present, lawyers seem to the principal researchers in this field. Information professionals are, however, particularly well placed to undertake research into user attitudes and into the interaction between electronic information and the law. For example, there continues to be a need for research into models of attitudes towards copyright and other legal issues, and into the effectiveness of filtering software. Such research might clarify the causes of the mis-match between users' priorities and government attitudes, and thereby help reduce the mutual misunderstandings that are present. Information professionals have always been the intermediary between the information and the user. This role should be expanded to becoming the intermediary between users and legislators, in particular, by shedding light on what people really want.

References

ArXiv (n.d.), available at: www.arxiv.org (accessed 12 May 2008).

Ayre, C. and Muir, A. (2004), "The right to preserve", *D-Lib Magazine*, March 2004, available at: http://dlib.org/dlib/march04/ayre/03ayre.html (accessed 12 May 2008).

Bailey, S. and Thompson, D. (2006), "Building the UK's first public web archive", *D-Lib Magazine*, January, available at: www.dlib.org/dlib/january06/thompson/01thompson.html (accessed 12 May 2008).

Bainbridge, D. (2003), "Trademark infringement, the internet and jurisdiction", *Journal of Information, Law and Technology*, available at: www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/bainbridge (accessed 12 May 2008).

Bakker, P. (2005), "File sharing – fight, ignore or compete?", *Telematics and Informatics*, Vol. 22, pp. 41-55.

Bigos, O. (2005), "Jurisdiction over cross-border wrongs on the internet", *International and Comparative Law Quarterly*, Vol. 54 No. 3, p. 585.

British Library (n.d.), "Analysis of 100 contracts offered to British Library", available at: www.bl.uk/ip/pdf/ipmatrix.pdf (accessed 30 June 2008).

Burrell, R. and Coleman, A. (2005), *Copyright Exceptions: The Digital Impact*, Cambridge University Press, Cambridge.

Burrull, A.L. and Oppenheim, C. (2004), "Legal aspects of the web", *Annual Review of Information Science and Technology*, Vol. 38, pp. 483-548.

Chartered Institute of Library and Information Professionals (n.d.), "Infoethics", available at: www.infoethics.org.uk/CILIP/admin/index.htm (accessed 30 June 2008).

Ciffolilli, A. (2006), "The economics of open source hijacking and the declining quality of digital information resources", *First Monday*, Vol. 12, available at: www.firstmonday.org/issues/issue9_9/ciffolilli/index.html (accessed 12 May 2008).

Collins, M. (2005), *The Law of Defamation and the Internet*, Oxford University Press, Oxford.

Covenant Eyes (n.d.), available at: www.covenanteyes.com (accessed 12 May 2008).

Cox, J. (n.d.), "Model standard licenses for use by publishers, librarians and subscription agents for electronic resources", available at: www.licensingmodels.com (accessed 12 May 2008).

Creative Commons (n.d.), available at: http://creativecommons.org (accessed 12 May 2008).

Cunningham, A. (2004), "Assessing the justification for rights management systems", *Journal of Information Law and Technology*, No. 3, available at: www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_3/cunningham/(accessed 12 May 2008).

Davison, M.J. (2005), *The Legal Protection of Databases*, Cambridge University Press, Cambridge.

DeHaas, R.J. (2007), "Access of internet use for a selected user", US Patent Application 20070061869, available at: www.freepatentsonline.com/y2007/006189.html (accessed 15 March 2007).

Derclaye, E. (2008), *The Legal Protection of Databases*, Edward Elgar, Cheltenham.

Deveci, H.A. (2005), "Personal jurisdiction: where cyberspace meets the real world I", *Computer Law and Security Report*, Vol. 21, pp. 464-77.

Deveci, H.A. (2006), "Personal jurisdiction: where cyberspace meets the real world II", *Computer Law and Security Report*, Vol. 22, pp. 39-45.

Directory of Open Access Journals (n.d.), available at: www.doaj.org (accessed 12 May 2008).

Directory of Open Access Repositories (n.d.), available at: www.opendoar.org (accessed 12 May 2008).

Durrant, F. (2006), *Negotiating Licences for Digital Resources*, Facet, London.

Eschenfelder, K.R. and Desai, A.C. (2004), "Software as protest: the unexpected resiliency of US-based DeCSS posting and linking", *The Information Society*, Vol. 20, pp. 101-16.

European Commission (2005), "Evaluation of database right", available at: http://europa.eu.int/comm/internal_market/copyright/prot-databases/prot-databases_en.htm#20051212_2 (accessed 12 May 2008).

Giavarra, E. (2001), *Licensing Digital Resources: How to Avoid the Legal Pitfalls*, Deutsches Bibliothekinstitut, Berlin.

Gillespie, T. (2007), *Wired Shut*, MIT Press, Cambridge, MA.

Gringras, C. and Todd, E. (2008), *Gringras on the Laws of the Internet*, Tottel Publishing, London.

Guibault, L.M.C.R. (2002), *Copyright Limitations and Contract*, Kluwer Law, The Hague.

Hann, G. (2003), "Liability in cyberspace", *Business Information Review*, Vol. 20 No. 2, pp. 95-101.

Harris, L.E. (2002), *Licensing Digital Content: A Practical Guide for Librarians*, American Library Association, Chicago, IL.

Hart, T. and Rolletschek, G. (2003), "The challenges of regulating the web", *Info*, Vol. 5 No. 5, pp. 6-24.

Hess, C. and Ostrom, E. (2007), *Understanding Knowledge as a Commons*, MIT Press, Cambridge, MA.

Hope, J. (2008), *Biobazaar: The Open Source Revolution and Biotechnology*, Harvard University Press, Cambridge, MA.

Internet Archive (n.d.), available at: www.archive.org (accessed 12 May 2008).

Jacobs, N. (2006), *Open Access: Key Strategic, Technical and Economic Aspects*, Chandos Publishing, Oxford.

Jaffe, A.B. and Lerner, J. (2007), *Innovation and Its Discontents*, Princeton University Press, Princeton.

Joint, A. (2003), "Online chatroom regulation", *Computer Law and Security Report*, Vol. 19 No. 1, pp. 44-8.

Jones, R., Andrew, T. and MacColl, J. (2006), *The Institutional Repository*, Chandos Publishing, Oxford.

Kavcic-Colic, A. (2003), "Archiving the web: some legal aspects", *Library Review*, Vol. 52 No. 5, pp. 203-8.

King, I. (2004), "Internationalising internet governance: does ICAN have a role to play?", *Information and Communication Technology Law*, Vol. 13 No. 3, pp. 243-58.

Kohl, U. (2007), *Jurisdiction and the Internet*, Cambridge University Press, Cambridge.

Legal Deposit Libraries Act (2003), available at: www.opsi.gov.uk/acts/en2003/2003en28.htm (accessed 12 May 2008).

Leith, P. (2007), *Software and Patents in Europe*, Cambridge University Press, Cambridge.

Lessig, L. (1999), *Code*, Basic Books, New York, NY.

Lessig, L. (2004), *Free Culture*, Penguin Press, New York, NY.

Lex [Column] (2006), "Music industry", *The Financial Times*, January 24.

Markel, M. (2002), "Deep linking: an ethical and legal analysis", *IEEE Transactions on Professional Communication*, Vol. 45 No. 2, pp. 77-83.

May, C. (2007), *Digital Rights Management: The Problem of Expanding Ownership Rights*, Chandos Publishing, Oxford.

NESLI (n.d.), "The model Nesli2 licence for journals", available at: www.nesli2.ac.uk/model.htm (accessed 12 May 2008).

Plotkin, R. (2003), "From idea to action: toward a unified theory of software and the law", *International Review of Law, Computers & Technology*, Vol. 17 No. 3, pp. 337-46.

Plotkin, R. (2005), "Software patentability and practical utility: what's the use?", *International Review of Law, Computers & Technology*, Vol. 19 No. 1, pp. 23-36.

Porsdam, H. (2006), *Copyright and Other Fairy Tales: Hans Christian Andersen and the Commodification of Creativity*, Edward Elgar, Aldershot.

Prins, J.E.J. (2003), "Consumers, liability and the online world", *Information and Communication Technology Law*, Vol. 12 No. 2, pp. 143-64.

Reed, C. (2004), *Internet Law*, Cambridge University Press, Cambridge.

Rowland, D. and Campbell, A. (2002), "Content and access agreements: an analysis of some of the legal issues arising from linking and framing", *International Review of Law, Computers & Technology*, Vol. 16 No. 2, pp. 171-86.

Rustad, M.L. and Koenig, T.H. (2005), "Rebooting cybertort law", *Washington Law Review*, Vol. 80 No. 2, pp. 335-416.

Saadat, M. (2005), "Jurisdiction and the internet after Gutnik and Yahoo!", *Journal of Information Law and Technology*, No. 1, available at: www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_1/saadat/(accessed 12 May 2008).

SHERPA (n.d.), "Publisher copyright policies and self-archiving", available at: www.sherpa.ac.uk/romeo.php (accessed 12 May 2008).

Spinello, R.A. (2002), "The use and misuse of metatags", *Ethics and Information Technology*, Vol. 4, pp. 23-30.

Sutter, G. (2003), "The UK and online intermediary liability", *International Review of Law, Computers & Technology*, Vol. 17 No. 1, pp. 73-84.

Tang, P. and Pare, D. (2003), "Gathering the foam: are business method patents a deterrent to software innovation and commercialisation?", *International Review of Law, Computers & Technology*, Vol. 17 No. 2, pp. 127-62.

Von Bernstorff, J. (2003), "Democratic global Internet regulation? Governance, networks, international law and the shadow of hegemony", *European Law Journal*, Vol. 9 No. 4, pp. 511-26.

Walsh, M.G. *et al.* (2003), "Marketers' book in cyberspace: the Anticybersquatting Consumer Protection Act", *Journal of Public Policy & Marketing*, Vol. 22 No. 1, pp. 96-101.

Web2Rights Project (n.d.), "Basic information about the IP and Web 2.0 landscape", available at: http://web2rights.org.uk/documents.html (accessed 30 June 2008).

Willinsky, J. (2005), *The Access Principle*, MIT Press, Cambridge, MA.

Corresponding author
Charles Oppenheim can be contacted at: c.oppenheim@lboro.ac.uk