Virtual liability

Julian Burnside, Q.C.

Introduction

The potential for legal liability on the Internet is enormous. To what extent the potential crystallises into reality depends on how the Net develops over the next few years.

Let me identify a few areas where the scope for liability is the least fanciful:

- defamation;
- breach of copyright;
- domain names;
- misleading and deceptive conduct.

Ancillary Issues

In any litigation which involves any of those areas of substantive law, there will be ancillary legal difficulties, in particular:

- evidence;
- jurisdiction;
- choice of forum and choice of law.

Although these issues are ancillary to the question of legal liability, they are capable of determining the outcome in a practical way: if it is all too hard, the stakes have to be very high to justify litigation. This may operate especially harshly when the litigants are unequally matched. This phenomenon is already familiar in orthodox computer litigation, and to some extent in general commercial litigation.

The Internet has created new paradigms for commerce, and so new problems for a legal system which grew out of older paradigms.

Where does an Internet transaction occur? If the claims of an Internet trader are false, do we apply the law of the place:

- where the trader carries on business; or
- where the trader's server is located; or
- where the misled customer is?

How to prove the content of a misleading page on the Web, if it has changed by the time its falsity is discovered? In all probability, it never was fixed in documentary form, and there is no central broadcaster to keep a log of all material "put to air".

Where to sue? If a citizen of Pakistan surfs to your site and suffers a loss because of your carelessness or breach of contract or misleading conduct, will they sue here or in Pakistan?

It is probably a safe bet that most people who use the Web for recreation or commerce are unaware that they are at the fringes of extremely difficult areas of international law.

Defamation

Let me make two preliminary comments:

- the relaxed and informal origins of the Net have encouraged a relaxed and informal mode of discourse, which increase the likelihood of defamatory comment;
- the courts have already dealt with a case of defamation on the Net. Reality may only be a special case, but it is an important one.

What makes the Internet significant in the field of defamation is that the defamatory word spreads further and faster than has ever been possible before. Wireless communication makes it possible to spread defamatory comments instantaneously, but the geographic reaches are restricted to the broadcast area. The telephone allows a defamation to be sent anywhere in the world instantly, but generally to a very limited audience (talkback radio is a limited exception). The print media enable defamatory material to be spread very widely but very slowly.

Internet has changed all that. Your mischievous remark can now be read simultaneously by millions of people, all over the globe, doing damage on a corresponding scale.

It might once have been thought that Internet was a bit of a club, and that a defamation action was not the done thing between members. Not so. **Rindos** v **Hardwick** dispelled that myth.

Here arises an interesting problem. It is well-known that the principles which guide defamation law in the United States are different from those which guide it in Australia and the UK. Other jurisdictions show different approaches again: the civil law jurisdictions adopt a different model from those in the common law jurisdictions. To take an example, the law relating to defamation in the United States is significantly affected by the provisions of the First Amendment, which guarantees a right of free speech. It is the First Amendment which justifies the bizarre excesses of Channel 23 in New York: excesses which would unquestionably amount to defamation in Australia.

Suppose then that an American puts on his or her Web page the contents of a Channel 23 program, which is critical of a visiting Australian politician. As broadcast in New York, it is justifiable. By virtue of being put on the Web it is readily accessible in Australia. Here it is defamatory. Has

it been published in Australia? If so, by whom? If it is published in Australia, does the rule in **Phillips v Eyre**[1] (which determines whether a cause of action is justiciable in another jurisdiction) prevent it from providing the foundation of an action in Australia for defamation.

These questions are difficult to answer, because the Internet has caused a paradigm shift which the law has not anticipated.

The only safe course is to assume that if you defame someone on the Internet, you can expect trouble: after all, litigation is trouble, even if you are wholly successful in defending it.

Of course, this is only the first layer of the problem - I have confined my remarks to the position of the author of defamatory matter. What of the service provider who "publishes" it?

Here too, the paradigm shift sends us in search of the right metaphor for legal liability. Is the service provider to be treated like the publisher of a newspaper, or like the newsagent who sells the paper, or like the distributor who carriers the paper to the newsagent? The service provider's role may have elements of each.

Let me put a hypothetical example. An American citizen creates a document called "All the Dirt on Australian Politicians". Its contents are true to its title. His own Web page is innocuously titled. His service provider does not read the contents of the home page, but simply allows him to use the server for the purposes of his home page. An Australian surfs to the site, and is enthralled to read what his political readers have been caught at: he hasn't seen any of that in The Australian! He includes on his own home page a link to that site. He renames his own home page "Political Dirt File". Apart from the link, nothing in his home page is defamatory. A large number of Australian politicians are embarrassed by the material which has quickly become the Cool Site of the week on a growing number of Australian home pages.

The problem does not readily yield to legal analysis. In **Rindos'** case[2], the defamation was written locally, posted locally and seen locally (eg, by the plaintiff) as well as elsewhere. It provides limited guidance to more complex possibilities.

On one view, providing the link is equivalent to publishing the libel locally. And yet if I say to a person "Ring this telephone number and you will learn some interesting and discreditable things about your political foes" there can be no suggestion that I have thereby defamed anyone. Which is the right metaphor?

The problem might be solved by reference to the balance between freedom of speech and the protection of personal reputations. But even that solution depends on choosing between competing models of free speech. There is no escaping the international flavour of the Internet; there is no reason to suppose that our own legal and moral models will be universally adopted.

One thing is for sure: if you injure the rich, powerful or sensitive, beware. See the **McLibel site** for a useful object lesson.[3]

Breach of Copyright

Copyright law is governed nationally. However, there are two international copyright conventions. Most countries in the world are signatories to one or both of them. Thus, more than in most other areas of law, there is a degree of uniformity in copyright law in most countries of the world. What is a breach of copyright in one place is very likely a breach of copyright in most other places. There are, of course, limited exceptions to this, but it is unwise to depend on those exceptions.

It is a fundamental principle of copyright law that the copyright owner has the exclusive right to do the various things comprised in the copyright. Those things include reproducing the work in a material form, performing the work in public and authorising any of the acts comprised in the copyright.

Where the subject matter of copyright is software, there seems to be an assumption that if something can be copied easily then it is alright to do so - why else would software manufacturers make it difficult to decompile their works. This is sometimes expressed differently - if the code is in the "public domain" then it may lawfully be copied. These are myths.

It is a breach of copyright to reproduce a work without the authority of the copyright owner. Computer programs, image files and data files are all copyright works. Downloading them involves reproduction in material form. It is an infringement of copyright unless done with the authority of the copyright owner.

The world of the Internet is awash with copyright material.

There are two principal copyright issues which will arise in an acute form on the Internet:

- whether the author of copyright material on the Net has, by implication, licensed the reproduction of the work;
- whether a service provider who makes an author's work available on the Net thereby authorises reproduction of it.

Implied Licence

Increasingly, authors are careful to place copyright notices on works placed on the Net, identifying precisely what use of the work is authorised. It is important that they do so. The Courts are slow to imply a licence to reproduce copyright works (see **Ipec v Time-Life Australia**[4]). Whether they will or not depends on an indefinite range of factual circumstances. It remains to be seen how well the Courts will understand the realities of the Net when assessing the circumstances relevant to an implied licence. This question is bound to emerge as a serious issue before long, given the amount of substantial software and other material available for downloading

on the Net and which, increasingly, is then distributed in a commercial or quasi-commercial context.

Authorising Infringement

It is a breach of copyright to authorise another person to breach copyright. This is a problem for service providers who make it easy for users to download copyright works. If the copyright owner has not licensed the copying of their work, then it is an infringement to copy it. If the service provider is held to have authorised the copying, then the service provider has also infringed copyright. Generally speaking a service provider will be a more attractive target in litigation than the anonymous individuals who download the copyright material.

The problem mirrors one which sent shockwaves through schools and universities some years ago. In **Moorehouse v University of New South Wales**[5], the High Court of Australia held that the university had infringed copyright by authorising students to make copies of copyright works. The acts of authorisation amounted only to this; that the university made available a photocopier in the library, which students were able to use for the purposes of making copies of portions of books. It was aware that students frequently made copies which were more substantial than qualified for fair use.

Since **Moorehouse's** case, educational institutions have taken various steps to deter students from making infringing copies, whilst permitting them to make non-infringing copies.

Does a service provider authorise copying? The answer will vary according to circumstances; but in many cases, the answer will be "Yes". There is substantial scope for service providers to be held liable for authorising infringement of copyright. They should make sure that they have permission to place on the Net the material which they do place there. More particularly, they should make sure that they have the author's permission to authorise the reproduction of the work.

There is another substantial issue in the area of copyright: will traditional notions of copyright survive in an age where an increasing number of works are never fixed in a material form as previously, and where information and ideas are increasingly the subject of commerce? It is beyond the scope of this paper to explore the issue. An excellent discussion of the problem can be found in The Economy of Ideas by John Perry Barlow.

Domain Names

Domain names are distinctive and useful; they are therefore potentially valuable. They are allocated by InterNIC, on behalf of IANA (Internet Assigned Numbers Authority), principally on a "first come first served" basis.

For any network to operate, each machine must have a unique designation. This is achieved by assignment of Internet Protocol Addresses (IP addresses) which have the familiar form 203.13.222.1. Numbers like that are OK for machines, but they don't leave an indelible mark in any but the most perverted minds. InterNIC associates chosen domain names with the site's IP address, so that a call for the name will be understood as a call for the associated number.

The general form of a domain name is **Lawnet.com.au**, in which the designators are representing organisation.type.country respectively. The organisation-designator will generally be chosen so as to be descriptive of the organisation or its products, or in some other was distinctive. The type-designator will depend on the nature of the organisation. Familiar type designators are .com for commercial, .gov for government, .edu for educational, .net for organisations operating a network, and .org for organisations which do not fit the other categories. It remains to be seen whether any greater credibility or cachet attaches to one or other type-designator. It is reasonable to suppose that a casual cybersurfer might be less alert for rip-offs on an .edu site than in a .com site. However, a domain name can be obtained in one capacity and retained as the nature of the organisation changes. In view of the increasing commercial drift of educational institutions and government instrumentalities, the domain name drift is probably no more than a reflection of reality.

The country-designators do not permit much fudging.

It is natural that organisations want domain names which are descriptive of the organisation or its site. It is likely that QANTAS airlines would be upset if Ansett obtained the domain name "qantas.com.au". Equally, they might be upset if the name was taken by the Fred Smith Travel Agency.

It will come as no surprise that such things have already happened on the Net.

Adam Curry was for a long time the presenter of the MTV program. As an adjunct to the program, he developed a website called "mtv.com". When he and his employer parted company, Curry continued to run his Website. The ensuing litigation was settled.[6]

Slightly more predatory was the behaviour of the editors of the Princeton Review. It is a company which prepares study materials for college students. Its principal competitor is the Stanley Kaplan Review. The Princeton Review registered with InterNIC the names "princeton.com" and "review.com". They also registered "kaplan.com"! Now, Kaplan did not have a presence on the Web. But he soon enough learned what Princeton had done. The litigation which followed resulted in Princeton being ordered to surrender rights to the domain name "kaplan.com". There were other features of Princeton's behaviour which call for comment and (depending on your disposition) censure or applause. First, they used the kaplan.com site to disparage the Stanley Kaplan Review, so adding insult to injury. Second, they offered at the outset to surrender the name in

exchange for a case of beer: an offer which Kaplan refused. Third, having been ordered to surrender the name, they sought to register the name "kraplan.com". Wait for the next round of litigation.

The legal issues are not novel. Similar problems have been met and dealt with in relation to telex addresses, at a time when the telex was the last word in modern communications. The general form of the legal solution lies in the common law of trade marks and passing off. In Australia, section 52 of the Trade Practices Act[7]. Speaking generally, a person will be restrained from using a domain name if that use is likely to deceive people into thinking that the site is associated with another person, or if the use of the name is otherwise likely to mislead or deceive.

In the USA, where telephone numbers can take the form of a mnemonic because the dial associates 3 letters of the alphabet with each digit, many businesses choose telephone numbers which spell out a word descriptive of the subscriber's business: UNITED-99 or PAN-AM-456 or HOLIDAYS. In New York (where else!) a call girl service advertises itself as 69-69-SEXY. Others are even more explicit. As a consequence, the US courts have a deal of experience in resolving disputes arising from predatory or misleading choice of telephone mnemonics. A similar solution is likely to be found for the similar problem of domain names[8].

Although the legal test can be formulated easily enough, it may be easier applying it when the disputed name is an invented name (Coca Cola, Exxon) or a distinctive personal name (Estee Lauder, Pierre Cardin) than when it is a common word or name which has acquired distinctiveness in connection with a particular product (McDonald's, Apple, Shell). In such cases, the problem becomes one of determining whether the distinctive connection extends to the Internet, and whether the disputed prior applicant for the name has some legitimate claim to it. No doubt difficulties would be encountered if an archery supplier registered "target.com" or an enterprising Scot registered the domain name "macintosh.computers.com".

Misleading and deceptive conduct

The problems arising out of the use of domain names dovetails naturally with a discussion of misleading and deceptive conduct. If the Net continues to develop in the way which presently seems likely, it will become a powerful force in commerce. It is a safe bet that where there is money to be made there are opportunities for the unscrupulous. For every credibility gap there is a gullibility fill.

The misleading use of domain names is likely to fall into one of the following categories:

- falsely suggesting a connection between the site and a known real-world business (kaplan.com; mtv.com; mallesons.com);
- falsely suggesting a connection between the site and particular goods or services (apple.repairs.com; sixty.minutes.com);
- falsely suggesting particular qualities or attributes (free.software.com; real.time.news.com); exploiting predictable mistakes of reading or typing (microfost.com; AZN.bank.com; symantac.com).

These are likely to find a legal solution which meets the merits of the case.

More difficult problems will arise out of misleading or deceptive material contained on web sites. First, how to prove the content of the site, which may have changed by the time the falsity is discovered? Second, can the server be sued for allowing misleading material to be put on the Net? Third, can a person be liable for giving a link to the site knowing it to contain false or misleading information?

Clearly the answer will vary in different jurisdictions. In Australia, the provisions of section 52 of the Trade Practices Act will govern the result. It is worth bearing in mind that it is not necessary that a person intend to mislead: it is enough that the conduct be in fact misleading or deceptive and causes damage.

A larger question is how and where to sue, if the person who maintains the site is in another country? International litigation is not for the faint-of-heart or light-of-wallet. It is not clear where the relevant behaviour occurs, if the site is maintained in one country, placed on the Net by a server in another country and accessed by a user in a third country via computers in any number of other countries.

1 **Phillips v Eyre** (1870) LR 7 QB 1: and see Breavington v Godelman 80 ALR 362; 169 CLR 41.

2 **Rindos v Hardwick**, Supreme Court of Western Australia, 31 March 1993, per Ipp J.

3 http://anthfirst.san.ed.ac.uk/McLibelTopPage.html.

4 (1977) 138 CLR 534.

5 (1974) 23 FLR 112.

6 See Rosalind Resnik, Cybertort: The New Era, THE NAT'L LJ, July 18, 1994, at A1.

7 Section 52 provides: "A corporation shall not, in trade or commerce in connection with the supply or possible supply of goods or services, engage in conduct which is misleading or deceptive or likely to mislead or deceive". The Trade Practices Act is directed at the behaviour of corporations in trade or commerce because of the constitutional limits of the power of the Commonwealth government. In several States of Australia there is legislation which makes similar provision directed at the behaviour of individuals.

8 See the very entertaining and informative article by Dan L Burk "Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks 1 U. RICH J.L. & TECH. I (April 10, 1995).

Julian Burnside QC is a member of the Melbourne Bar.