

CYBERLAW CONFERENCE

NAME AND REPUTATION IN THE FOURTH DIMENSION

by

Shane Simpson

SIMPSONS SOLICITORS

Sydney Hilton

Wednesday 1st April 1998

Part A: The Protection Of Name And Reputation In Cyber-Commerce

Part B: Component / Application Authorship And Other Software Issues.

PART A

THE PROTECTION OF NAME AND REPUTATION IN CYBER-COMMERCE

Name and reputation is a core asset of every business and the most common strategy for the protection of that asset is the registration of trademarks. It is the legal mechanism for branding products so that they are immediately identifiable with their corporate source. It provides reassurance to the customer as to style and quality and is an effective tool by which the owner of the mark can stop others from unfairly appropriating its brand value.

In the digital environment branding is going to be even more important than in the traditional, atom-based, commercial world. Given the cacophony on the Internet, one of the most valuable tools any copyright owner will have is a brand which will attract the market to its web site. "Creepy crawlies" and "bots" may be your best friend but if you are looking to buy something particular, you are likely to prefer to go straight to where you know you'll find it. If you wanted to buy a particular Phillip Glass album, would you be more likely to buy it through the Sony Music homepage or from a no-name company using a post box out of Finland? If you want to buy a Mickey Mouse T-shirt you will be heading off to the Disney page without much further thought.

Quite simply, people will be more likely to use an unfamiliar medium for commerce if they are dealing with people or things that they trust. That is what brand recognition is all about. And that is why trademarks are going to be central to the commercial life of cyberspace.

As it has always done every time a new technology requires it, intellectual property will adapt to its new technological environment. That said, because the applications and capacities of digital technology expand in ways and degree that only the futurists might guess, there are, for the moment, more questions than answers in this field.

Today, I want to focus on the **commercial ramifications of intellectual property in cyberspace**. In particular I will focus on trademark. I want to emphasise the commercial aspects of the topic rather than enter a legalistic analysis of the evolving case law because it is the commercial issues that interest our corporate clients. They are the ones that subscribe to services such as Forrester Research Inc (www.forrester.com) to find out the latest demographics of cyber world; to find out the ways in which they are going to have to modify the way that they do business.

All corporations are, not surprisingly, motivated by protecting their core business assets, promoting the value of those assets and expanding their territory of sales and thus their market share. It is a brave managing director who simply dismisses cyber world as an important emerging marketplace. Accordingly, one of the greatest challenges faced by executives is whether they try and move their existing business into the cyberspace environment, and if so, how best to adapt to the conditions of this new market territory.

For most corporations undertaking these early exploratory forays into cyber world, Intellectual Property is already an important part of their balance sheet. For many, it is their core business. For all, it is fundamental to their branding, marketing, promotion and sales success.

Thus, the question that all corporations should ask of their Intellectual Property lawyers is, or should be:

" How should we use Intellectual Property in protecting and promoting our business in cyber world? Have we achieved best practice in this new environment?"

Nobody knows the answers yet. Its just that some of us are doing more future gazing than others. Our corporate clients expect us to be creative in solution finding but this is an area in which there are not yet a lot of solutions. Our creativity is better proven by development of preventative strategies. In cyberspace the key role for Intellectual Property lawyers is prevention - because cure is often much more difficult and expensive.

Stakeholders

Let us begin by identifying the stakeholders. We must do this so as to identify and meet the challenges they face.

They include:

(i) **companies** that have developed value in their **name and reputation**

All successful companies recognise the importance of enhancing and protecting their individual identity. Name and reputation is a key element of branding, marketing and promotion. No such company wishes to endanger the existing value of their corporate or brand identity. If its involvement in e-commerce means that this may be damaged, there will be enormous reluctance to become involved. On the other hand, if it is more likely that damage will occur because they are not involved in this new marketplace, they will be forced to commit themselves and develop a strategy that is at least protective, even if it is not aggressive.

(ii) **companies** that have developed value in their **copyright interests**

These include many of our largest corporations such as newspapers, radio and television stations, publishers, record and music publishing companies, software and hardware companies, technology-based companies and so on. These companies are having to become involved whether they like it or not. The Internet is really just a massive content distribution system. Given that technology makes it difficult to stop third parties from making proprietary content available on the Net, the best way of protecting that content is to become the most obvious and reliable source of it. If content-driven corporations don't, they will lose control of their primary assets and within a generation, they will have disappeared.

(iii) **customers** who rely on the corporate identification

These are widely regarded as the weakest players; they are traditionally failed by the market place and there is even greater cause for concern in cyberspace where unequal access to information further disadvantages this class of eager new inhabitants of cyber world.

(iv) **potential users of copyright information**

The IT environment is supposed to have delivered a miracle of access to information. It has: to both the valuable and the rubbish; the copyright protected and the public domain material. Access has never been easier and nor has the ability to copy, amend, adapt, publish and republish. This group too, will be drawn by corporate and product branding to assist them in sieving the wheat from the chaff. (I have already used an example of this in this paper - a reference to the Forrester Research Inc web site rather than relying on, say, a web chat group.)

(v) **individual creators** of copyright material

These have adapted to the new environment like frogs in a swamp. Cyber world is populated by millions of individuals who see the Internet as a way of publishing their creative efforts to others. They can bi-pass the traditional information distribution systems. They can get their creative material out there and, who knows, someone might see it and instead of stealing it, might acknowledge them, even if they don't pay for it. In spite of their essential role, individual creators have always been at the bottom of the copyright food chain and their position is no different in cyber world.

(vi) **society at large**

The community has a benefit in both achieving access to a wide selection of information, balanced against the societal interest in promoting the creation of new work. The health of a society, it may be argued, can be judged by the balance that it achieves in meeting these related, but sometimes competitive, interests.

If any cyber world copyright regime is going to be successful, it must meet the needs and expectations of all of these stakeholders. If it only looks to the needs of some of them, it is unlikely to be successful because each has the ability to revolt and demand change. That said, in this paper I will focus only on the first stakeholders: companies that have developed value in their name and reputation. However, the other stakeholders will and must,

maintain a subliminal presence throughout the whole discussion.

OVERVIEW OF THE ISSUES

One of the principal ways that business protects its name and the reputation that attaches to its products and services, is through the trademark system. It is perhaps trite to say, but it is important nevertheless:

- (a) that trademark is nationally based and thus the owner of a mark in Australia is not protected against those who use that mark outside that jurisdiction. It is powerful within the jurisdiction of registration and essentially impotent outside it; and
- (b) that because the Internet has no national boundaries, when a company enters cyber world, it is engaged in a business environment that is, by definition, international. However it does so using a system to protect its name and reputation that is based on national boundaries - a system that works well in one environment but is simply not designed for the new one.

One current example of this is the clash between owners of trade marks and owners of domain names.

DOMAIN NAMES AND TRADEMARKS

Introduction

(For a history and technical background of domain names, see Robert Shaw, Internet Domain Names: Whose Domain Is This? at "What is the Internet domain name System," <www.itu.ch/intreg/dns.html>).

The domain name is one of any company's critical assets because it is how its customers and potential customers will identify, find and contact the business.

If you see the address "**coke.com**" do you not immediately think of Coca Cola? Is it not an obvious address for the giant bottler? If you wanted to visit the NASDAQ wouldn't you think that typing "**nasdaq.com**," would be the most likely address? of course. Unfortunately the owners of those marks in the atom-based environment failed to register them as domain names - (they had to acquire them later!). If trademark is the principal tool for the protection of corporate identity and the domain name is the most important corporate identifier on the Net - what sort of legal advice were these organisations getting. Clearly, not very proactive service.

The potential for conflict is obvious. It is a potential that is already being realised. Due to the lack of legal clarity and government policy direction, the conflict between domain name identifiers and trademark has given rise to one of the most important and controversial issues in cyber law.

As you all know, there are four main ways that the law provides protection of business names and reputations: trade mark; copyright; passing off; and ss.52 and 53 of the Trade Practices Act. These are powerful tools in the atom-based business environment but do they give adequate protection to the competing interests doing battle in cyberspace?

The legal status of domain names

Once you secure a domain name you have the 'web rights' to it across all countries and all classes of goods and services. Even so, the legal status of domain names in Australia is uncertain. Are they like trademarks, a source of origin or identity and, thus capable of being owned, or are they really analogous to street addresses?

What sort of property is a domain name?

What sort of rights should it attract?

Should it be dealt with as a trademark or as some other form of property?

The administrative authorities responsible for allocating domain names have paid little attention to these issues, handing out names on first come first-served basis, until they became embroiled in litigation. (Now some such as InterNIC require written indemnities from applicants.) As a result, these authorities have established (arguably inadequate) dispute resolution procedures, which generally provide that when a dispute arises, if the trademark owner can prove its registration within 30 days, the domain name is suspended until the dispute is resolved by court order or settlement.

For example, when NSI put Roadrunner Computer Systems' domain name, "**roadrunner.com**" on hold because of a challenge from Warner Bros., it found itself the subject of a lawsuit. This case highlights the failure of NSI's policy to take into account the cornerstone of trademark infringement analysis: "likelihood of confusion" But can an essentially administrative authority be held responsible for what really amounts to a fundamental flaw in the intellectual property paradigm when dropped into a cyber-context?

See also Data Concepts Inc. v Digital Consulting Inc. and Network Solutions Inc. (No.3-96-0429, M.D. Tenn. filed May 8, 1996) in which an inequitable situation arose where the party who actually had superior trademarks rights based on seniority of use, was forced to relinquish the domain to the junior trademark user who had the foresight to register the mark.

Can the domain name be used as a trademark?

The answer is a clear , "Yes". It's just like any other mark; it may acquire trademark rights through use, but for obvious reasons, registration is the safest option. It can be used as a trademark if it indicates the source and origin of goods and services - irrespective of the medium by which those goods or service are offered for sale.

If a business wishes to register its domain name as a trade mark it will be eligible provided that it is intended to be used as a trade mark, and if the name is sufficiently distinctive. In other words, the usual tests apply.

Merely using it as one's electronic street address would not fulfil this requirement as it is not using it as a trademark. There is insufficient link with one's goods and services.

Can a domain name use a phrase that is not allowed to be a trademark?

The domain name <**sydney2000.net**> was registered by an Internet service provider, Asia Pacific Internet Company. The Sydney Organising Committee for the 2000 Olympic Games sent a cease and desist letter, and has threatened proceedings. Commercial use of the phrase "SYDNEY 2000" is expressly prohibited by the Sydney 2000 Games Indicia and Images Protection Act 1996. If litigated, this would perhaps be resolved as a bare matter of statutory interpretation but if not, it is obvious that the case will have very important implications for the status of domain names in cyberspace.

What if someone else has an identical mark registered in a different class - who has rights to the domain name?

One of the greatest problems posed by trademarks in cyberspace arises when we move away from cases involving the very famous marks (like **Harrods**), or greenmailers (like **Toysareus**), or comedians (like **Princeton Review**), and have to advise combatants which are both just ordinary companies trying to carry on their bona fide businesses in this new environment.

For example when Prince PLC, in 1995 a British computer services company, obtained the domain names <**prince.co.uk**> and <**prince.com**>. When the Prince Sports Group, Inc., a well known U.S. manufacturer of tennis rackets, tried to register the domain, it couldn't. It already had several other domain names, including <**princetennis.com**> and <**princesportsgroup.com**>, and both parties commenced a flurry of cases over the right to the key, most obvious name. There was no bad faith and the courts did not find accede to the sporting company's demands. The English company won the UK case whereupon the parties settled the US case. Prince PLC still retains ownership of the domain.

Similarly, in the TechYard case, (Giacolone v. Network Solutions Inc., No. C-96 20434 RPA/PVT (N.D. Cal. June 14, 1996), the domain name "**ty.com**" stood for both "TechYard," the name of the site, as well as the domain name holder's son, Ty. The domain holder commenced proceedings to prevent Ty, Inc. from asking Network Solutions, Inc. (the organisation that issues domain names) to shut off "ty.com." (<<http://www.ty.com>>).

In these cases, our traditional notions of the monopoly rights created by trademark registration are certainly being challenged for in such cases, both parties are innocent players caught up in the unknown dimensions of the World Wide Web. There isn't a simple solution.

The difficulty posed by this situation illustrates either the limitations of trademark law in a cyber context or the incapacity of Internet Name Administrators to develop a system which respects and conforms to the Trade marks paradigm. To date, Name Administrators have been unable to develop a workable system which enables identically named businesses to distinguish themselves so as to avoid confusion for the consumer. Their approach is a simple one: if both parties with an identical name can show an equal level of ownership, (ie, TM registration), then the Domain Name will be given on a first come first served basis.

This administrative approach ignores the development in the legal framework to give enhanced rights to famous marks and, to some extent puts the famous and the little known on a fairly even footing: the fastest wins.

Can the same name be registered in different domains?

The problem caused by registering the word "apple" in the .com domain and also in the .asn domain is very likely to be confusing when one registrant is found to be a computer company and the other, a fruit growers association. However there is nothing in the domain name allocation system to prevent this.

Perhaps these problems will always arise, from time to time, given the paucity of the descriptors available in domain name language.

Can a domain name infringe a trademark?

This is the most commercially important question of all. Quite clearly, ss 52, 53 and s.120 of the Trade Practices Act and the common law of passing off, all show that a domain name can infringe a trade mark if the use is 'misleading or deceptive' or is 'likely to cause confusion'.

The focus of the decided cases is clearly on "likelihood of confusion" principles. The "likelihood of confusion" is the leitmotif that runs through all of them.

There is no doubt that a person will be restrained from using a domain name if that use is likely to mislead or deceive people into thinking that the site is associated with another company.

Likelihood of being confused or misled

"The confusing or misleading use of domain names can be identified by asking the following questions:

- (i) Is there a false suggestion of a connection between the site and a known third party business (**kaplan.com; mtv.com**)
- (ii) Is there a false suggestion of a connection between the site and a well-known third party
- (iii) Is there a false suggestion of a connection between the site and third party's goods or services (**lotusmotorcars.co.uk** cf **lotuscars.co.uk**)
- (iv) Is there a false suggestion of particular qualities or attributes (**free software.com; real-time-news.com**);
- (v) does it exploit predictable mistakes of reading or typing (**microsoft.com; micros0ft.com**).

These sorts of situations are likely to find a legal solution based on the merits of the case.

That said, proving that there is such a likelihood of confusion is not necessarily simple. For example, under the test formulated in Taco Co of Australia Inc v Taco Bell Pty Ltd (1982) 42 ALR 177 the conduct must contain or convey

some form of "misrepresentation" in order for it to be considered misleading for the purposes of s.52.

Role of s 120(3) of the Trademarks Act

Section 120 (3) of the Trademarks Act- introduced to enhance the protection of famous marks - is a particularly important provision - not just because of the powers it provides but for the future course it indicates. This provision gives protection to famous marks from substantially identical marks being used in unrelated classes of goods and services.

It is important not only because of the protection that it gives to famous marks per se but rather because, when we observe how the anti-dilution laws are developing in the USA, we can see that this may point to the direction that future legislative developments may take in order to meet the new demands of the cyber world.

The present system of classification of trademark registration and protection is of questionable efficacy in an environment in which the principal customer identifier (the domain name) is so potentially ambiguous and confusing.

That s.120(3) gives protection for marks that are well known in Australia against the use of substantially identical marks in unrelated classes of registration shows that the rigidity of the classification system is drawing nearer to its use-by date. This provision will be one of the most fertile areas of litigation in the protection of corporate name and reputation in the cyber-environment.

This provision, together with the recent anti-dilution US cases, suggests a significant shift in trademark protection, to a different analytical base.

This shift clearly favours the established players as it confirms that the value of one's trademark is not just based on registration but, more importantly, on the reputation that it represents. In brief, s.120 (3) and the 1995 Trademark Dilution Statute in the USA, both acknowledge:

- (i) the inherent association of the monopoly right and reputation;
- (ii) that reputation spills into areas other than the narrow classification of goods or services in which that reputation had been earned;
- (iii) that there is a high likelihood of "confusion, mistake or deception" when the reputation of a mark is appropriated by a third party - whether or not they are in direct competition;

In other words, we have recognition that the old category-based trademark regime is no longer sufficient to protect the ability of a famous mark to identify, distinguish and protect the reputation attached to the goods or services that it represents.

And in the meantime...

Until a new legislative and administrative paradigm is introduced, the courts must find rational approaches to resolve these conflicts. Thus, there is likely to develop a series of judge-made indicators to assist resolution, using extensions of existing principle.

For example in a Dutch case, the domain name <xxlink.nl> was held not to infringe the other party's rights to the XLINK Trademark. The court found that there was insufficient similarity in the services offered by the respective companies to give rise to confusion.

This reasoning of the case is in line with the traditional trademark paradigm of 'goods and services' classification but the approach is significant because, in looking to the nature of the services offered by the companies in dispute, the court assigned to the consumer a capacity for discernment and a degree of responsibility for service identification.

This might go some way to explain the Court's rationale in the Candyland case: Hasbro, Inc v. Internet Entertainment Group, Ltd., Case C96-130WD (WD Wash. filed January 26, 1996). In this example, the two classes of "confused consumers" were either children or perverts, neither of which could apparently be trusted to make a discerning judgement.

In that case, Hasbro obtained a restraining order against the operators of the Candyland website (a sexually explicit site) on the basis that it infringed Hasbro's Candy Land trademark (used in relation to children's toys). In an emotive case such as this one, where children would be unwittingly pulling porn off the net, it is not exactly clear what the court's true rationale was. The court ordered that the porn company cease and desist and hand the name over to Hasbro. <www.candyland.com>.

Another indicative factor may be whether the defendant has deliberately tried to cause confusion between the two parties to the proceedings.

In Planned Parenthood federation of America, Inc v Richard Bucci, d/b/a Catholic Radio, 42 USPQ 2d 1430 (S.D.N.Y. 1997), the defendant, an anti-abortion activist, admitted that he had chosen the domain name with the intent to divert Internet users who were seeking Planned Parenthood's web site to his own competing site. His site <www.plannedparenthood.com>, carried an opening banner that read, "Welcome to the PLANNED PARENTHOOD HOME PAGE" and promoted an anti-abortion text called The Cost of Abortion. Planned Parenthood, which owned the registered mark PLANNED PARENTHOOD, which it had used in connection with its reproductive health services for 50 years.

This raises another interesting issue - the role of motive.

Is motive significant?

(i) The homage or hurt sites

If you represent a well-know Sydney radio personality like John Laws, you would by now have registered the name "johnlaws.com.au" and various of the most obvious possibilities.

The last thing Mr Laws would want is for someone to set up a fan-club site using the address "lawsy.com.au".

It also raises the interesting spectre of a Laws competitor registering the domain name "johnlaws.com.au" and using it to put up stories that may be abusive of or hurtful to, the 'golden tonsils'.

In order to prevent this, even if Mr Laws was not intending to have a web-site of his own, would it not be wise of him to undertake some preventative work? It is a much cheaper strategy in the long run than trying to close down the offending site down or acquiring the rights to the site afterwards.

The Princeton Review case is an amusing example of this serious issue, (The Princeton Review Management Corp. v. Stanley H. Kaplan Educational Centre, Ltd., 94 Civ. 1604 (MGC)(S.D.N.Y., filed March 9, 1994).

Princeton Review is a publisher of study materials. Its main competitor is a company called Kaplan. Princeton registered "**kaplan.com**" and offered at the outset to surrender the name for a case of beer. (An example of ego-mail rather than green-mail.) When this offer was turned down, they then used the Kaplan site to disparage Kaplan. When the Court ordered them to surrender the name they sought to register "**kraplan.com**", the results of which are not yet known.

But what the court-ordered arbitrators failed to deal with, (and what has not been dealt with by the courts), was Princeton's subsequent establishment of the e-mail address "**kaplan.sucks@review.com**".

Whether they are doing it cynically or merely as a creative exercise, should people be prevented from anticipating popular, or useful names, registering them and then offering them for sale?

(ii) Parasites

Parasites expect to gain financially through actually using the domain name. This takes various forms but the theme is common: a company that is either a direct competitor or someone who wishes merely to trade of the name of another, registers a famous name or a mark that is similar to, or a commonly mistyped version of a famous name.

These businesses differ from cyber-squatters because they intend to use the name for their own purposes.

For example in the decision, Cardservice Int'l, Inc. v. McGee, 950 F. Supp. 737 (E.D. Va. 1997), the court found

infringement of the plaintiff's registered CARDSERVICE INTERNATIONAL mark for credit card and debit card processing and related services. The defendant, Webster McGee, had registered the domain <cardservice.com> and set up a web site advertising credit card processing services using the name "EMS - Card Service on the Caprock." In that case the court found that the evidence indicated that McGee's behaviour was "malicious," and granted a permanent injunction against him. So the court did not have to find on the rather more difficult point of whether Mr McGee would have had the right to construct this business activity if he was doing so in innocence. Clearly, bad motive was determinant.

(iii) Greenmail / Cyber-squatting

One practice that is causing many problems is the practice of taking well-known trademarks and registering them as domain names thus depriving the owner of the mark for their use as an electronic address. These people are often referred to as "squatters" or "cyber-squatters". They speculatively register domain names with the intention of selling them for profit. This practice has led to the emergence of "domain name brokers." (See <<http://www.bestdomains.com>>; <<http://www.domain-registration.com>>; <<http://www.domainmart.com/book/4sales.html>>.

For example...

If you have a business called Sydney OnLine you will prefer to have the electronic address of "**sydneyonline.com.au**". This would be easier for your potential customers to find than, say, "**sol.com.au**".

Given this, it is not surprising that there are many bottom-feeders who make a business out of searching the lists for valuable trademarks that have not been registered as domain names, registering them and then contacting the owner of the mark and offering the domain name for sale. This is just another form of the greenmail business.

In the Toys R Us Case, (Toys "R" Us, Inc & Ors v Eli Abir & Ors. 97 Civ.8673 (JGK) 1997), it was clear that the defendant was trying to bribe the plaintiff's over their rights to the "deceptively similar" domain name "**toysareus.com**", thus capitalising on what was likely to be an easy consumer mistake.

When the plaintiff's refused to buy the 'deceptively similar' domain name from him, he threatened to use the domain to operate a toy store catalogue and began soliciting business from toy companies in China.

The Judge described these actions as a "bad faith attempt at cyberpiracy", and the case was decided with "a presumption of confusion", (because it was admitted by the defendants), and a reliance on the new anti-dilution legislation in the US which will be discussed further below.

In Panavision Int'l v Toeppen 945 F.Supp 1296 (CD Cal.1996), where the facts were substantially similar, the court found against the defendant's attempts to "trade on the value of marks as marks". Toeppen had been in the business of registering famous marks as domain names and then holding their owners to ransom on the basis that

it would be cheaper to settle than to sue. He was not alone in this 'business venture'. An American journalist, Joshua Quittner published an article on this issue over the Net and then surrendered "mcdonalds.com" to McDonalds when they agreed to pay \$3,500 towards computers at a local school. (See Joshua Quittner, Billions Registered, WIRED, Oct. 1994, at 50, <<http://www.hotwired.com/wired/2.10/departments/electrosphere/mcdonalds.html>>.)

The practice is known as 'warehousing' or 'squatting' and in Australia too, this has become a petty industry. Certain individuals are becoming quite well known for searching the trademarks register, checking the domain name registers and reserving the obvious domain names. They then contact the unsuspecting companies and offer to sell the name back to them. This is a doomed business. As yet there are no Australian cases on point but there are now two important cases in England that point the likely direction of the Australian courts.

In Harrods v UK Network Services Limited et al., 1996 H 5453, Harrods was registered in the "co.uk" domain. The defendants registered the Harrods name in the American ".com" domain. The court held that use of the ".com" domain name by anyone other than the Harrods constituted trade mark infringement and passing off.

Perhaps the most important case in this area is the recent decisions of Marks & Spencer, Ladbrokes, J. Sainsbury, Virgin Enterprises and British Telecom v One In A Million [see 28th November (1997) Ch 1997 M.5403; L.5404; J.5402; V.5401; B.5421 respectively].

All of the plaintiffs have very famous names but had failed to undertake a program of defensive registration of domain names. The defendants are dealers in Internet domain names. They register names or trademarks of well-known enterprises and sell them to potential users. Clearly it is done without the permission of those enterprises. These registrations included the following:

britishtelecom.co.uk	cadburys.com	macdonalds.co.uk
bt.org	cellnet.net	macdonalds.com
britishtelecom.net	globalmedia.co.uk	motorola.co.uk
bskyb.net	j-sainsbury.com	marksandspencer.co.uk
burger-king.com	ladbrokes.com	marksandspencer.co.uk
burgerking.co.uk	leedsunited.com	marksandspencer.com
buckinghampalace.org	marconi.com	nokia.co.uk
personalnumber.co.uk	spice-girls.net	tandy.co.uk
j-sainsbury.com	spicegirls.com	tandy.net
sainsburys.com	spicegirls.org	thetimes.co.uk
sainsbury.com	sundaytimes.co.uk	virgin.org

None of them were active sites. They were simply names registered by the defendants and available for such use.

As the judge in that case pointed out, for a dealer in Internet domain names there are only four uses to which the names can be put:

- (i) "The first and most obvious is that it may be sold to the enterprise whose name or trademark has been used, which may be prepared to pay a high price to avoid the inconvenience of there being a domain name comprising its own name or trade mark which is not under its control."
- (ii) "Secondly, it may be sold to a third party unconnected with the name, so that he may try to sell it to the company whose name is being used, or else use it for purposes of deception."
- (ii) " Thirdly it may be sold to someone with a distinct interest of his own in the name, for example a solicitor by the name of John Sainsbury or the government of the British Virgin Islands, with a view to its use by him."
- (iv) "Fourth it may be retained by the dealer unused and unsold, in which case it serves only to block the use of that name as a registered domain name by others, including those whose name or trade mark it comprises. "

The court had no trouble finding that a tort had been committed.

"The essence of the tort of passing off is a misrepresentation to the public (whether or not intentional) liable to lead them to believe that the goods and services offered by the representor are those of the Plaintiff. However, the tort is also committed by those who put or authorise someone to put an 'instrument of deception' into the hands of others. 'No man is permitted to use any mark, sign or symbol, device or other name whereby, without making a direct false representation himself to a purchaser who purchases from him, he enables such a purchaser to tell a lie or to make a false representation to somebody else who is the ultimate customer: Singer v. Loog (1880) 18 Ch.D. 395, 412, cited with approval by Lord Macnaughten in 'Camel Hair Belting' [1896] AC 199, 215-6."

This is in line with the judgment in Direct Line Group Limited v. Direct Line Estate Agency [1997] FSR 374 where similar facts were described as "only reasonably consistent with an intention on their part to hitch themselves to other companies reputations and make an illicit profit by doing so'.

See too Glaxo Plc v. Glaxowellcome Limited [1996] FSR 388 where the court held that it "will not countenance any such pre-emptive strike of registering companies with names where others have the goodwill in those names and

the registering party demands a price for changing the names".

The interesting observation in the Marks & Spencer case was that the "mere creation of an 'instrument of deception', without either using it for deception or putting it into the hands of someone else to do so, is not passing off. There is no such tort as going equipped for passing off. It follows that the mere registration of a deceptive company name or a deceptive Internet domain name is not passing off."

That said, His Honour found that it was -

"beyond dispute that what is going on is calculated to infringe the Plaintiff's rights in future. The name "marksandspencer" could not have been chosen for any other reason than that it was associated with the well known retailing group... Where the value of a name consists solely in its resemblance to the name or trade mark of another enterprise, the Court will normally assume that the public is likely to be deceived, for why else would the Defendants choose it? In the present case, the assumption is plainly justified. As a matter of common sense, these names were registered and are available for sale for eventual use. Someone seeking or coming upon a website called <http://marksandspencer.co.uk> would naturally assume that it was that of the Plaintiffs."

"Any person who deliberately registers a domain name on account of its similarity to the name, brand name or trade mark of an unconnected commercial organisation must expect to find himself on the receiving end of an injunction to restrain the threat of passing off, and the injunction will be in terms which will make the name commercially useless to the dealer."

As to the trademark aspects of this litigation, the defendants had but two arguments: (i) they denied that their use of it has been 'in the course of trade'; and (ii) they contended that it is an implicit requirement of the Act that there should have been a likelihood of confusion on the part of the public, and that there had been none.

The judge had no trouble finding that the use of a trade mark by a professional dealer for the purpose of making domain names more valuable and extracting money from the trade mark owner was a use in the course of trade. [See British Sugar Plc v James Robertson & Sons Ltd. [1996] RPC 281, 290-2]. He did not find on the second point.

SUMMARY OF ADVICE TO CLIENTS

Given the above, how should we advise our clients so that they will be more likely to avoid the sorts of problems that are readily foreseeable. The following outlines a minimum strategy for proactive protection:

1. Owners of existing trademark should attempt to register their trademarks as domain names whether or not they intend to be involved in e-commerce.
2. They should select a domain name that exactly matches one of the company's registered trademarks, or reverse the process and obtain a trademark registration that exactly matches the business' domain name.
3. If the business has a distinctive domain name, it should use the domain name as a trademark for either goods or services and register that domain name as a trademark.
4. When registering the domain name, the business should ensure that it registers any other names, which customers may associate with the business.
5. Corporations intending to register trademarks should undertake domain name searches at the same time as they do the usual searches prior to trademark registration. They should then register the domain names at the same time as they file the trademark applications.
6. If a business is adopting a domain name, which is not an existing trademark, consideration should be given as to its likely strength or weakness as a trademark. After advertising and promotion, the domain name may be registrable as a trademark (eg the usual issues of whether the name is descriptive of the goods or services or whether it is a coined word or phrase).
7. Full searches, both Australian and international, should be performed before selecting a domain name. The searches should be international, if the business is intended to be conducted internationally.
8. No business should allow itself to be subject to greenmail demands from domain name warehouses. Preventative measures are much cheaper and more effective even though a mark owner is likely to win litigation undertaken in order to recover use of its name in cyberspace.

LINKING, TAGGING AND STUFFING

If we recognise that the reputation, which attaches to a mark also attaches to the company which owns that mark, we must acknowledge that reputation is an important corporate asset. Thus, we will realise the significance of new Internet technologies, which provide novel ways to appropriate the value of a third party's reputation. Internet innovations such as **Hotlinking** or **Hypertext Linking, In & Out**, permit us to connect our site to those of others - with or without their permission. When the user clicks on an icon or hypertext reference link, the link instantly takes the user to the new reference. It may be somewhere within the same site or it may be to someone else's site. The user does not know except that the URL address in the browser will change.

The hypertext link effectively allows each document to act as a by-pass to access other documents. These links allow users to spontaneously choose their route through information and destroy the traditional, more linear, path. The hot-link is both an essential navigational tool for the user and, for the linked-site, an important means of attracting visitors, hits, customers. This is valuable not only for the owners of the website content but also for the advertisers who chose to advertise on that web-site.

Some would argue that the more third parties provide a path to one's own site, the better.

In any event, "Hotlinking" is fundamental to the Internet and is an essential feature of Internet commerce. Because of this, there has developed an argument that there is an implied licence to provide links from your site to that of others. If there is such a licence it can only be to provide a link to the front door of the third party site and not to link directly to the interior of it. If it were otherwise, the rights owner and its advertisers would lose the commercial benefit of their site content.

In contrast, so-called "**image links**" bring an image contained in a separate file onto the page being viewed. The separate file may be an image file stored on the same server as the link or an image file stored on a separate, unrelated site. This is known as "linking in." This allows the original site owner to appropriate the content of another's site and incorporate it into his own site as though it was his own.

By means of "**framing**" the third party simply avoids all of the valuable corporate branding and all of the advertising that funds the facility, and appropriates the content without the permission of the owner and without any reward or compensation to it. It permits entire web pages to be captured from another site and placed in a window on the original site. This can be advantageous for the user, whose surfing may be shortened by the process but it destroys the corporate value of the site from which the information has been appropriated. Neither user nor original owner are notified of what is happening.

This process affects the very viability of e-commerce. The value of branding is diminished; customer loyalty is abused; it diverts potential customers from your site; and the value of advertising - one of the primary sources of cashflow for many web sites - is negated. It even affects the way we evaluate a site by the number of "hits" that a page receives for by framing and image linking, the usual counting mechanisms are by-passed.

Because of this, several web site owners are seeking legal remedies to protect their asset and it is not surprising that the trend of recent cases suggests that the websurfers' interest in ease of access is not being allowed to overwhelm the owners' rights to protect the corporate value that they have developed in their name and reputation as well as their content.

These cases are being argued using the usual old quiver of weapons - but particularly the Trade Practices Act. Common to most, is the argument that the linking of one site to another involves a representation that the linking site is in some way authorised by, or associated or affiliated with the linked site. As we know, the validity of this

argument is always determined by the facts of the individual case. But what standard of consumer or user awareness should be used when applying 'likelihood of confusion' tests? Does any net-surfer really think that a link from one site to another indicates authorisation, association or affiliation?

Up to now, the most likely answer to this question is a clear, "No". Net-surfers have been an elite highly educated user group, which have understood that cyberworld is an environment of absolute caveat emptor. Its early inhabitants have treated it as a lawless zone, where no person or information can be trusted but there are no locks on any doors.

The two key cases are [Ticketmaster Corp. v. Microsoft Corp](#) 1997 (No.97-3055 DDP (C.D. Cal. filed April 28, 1997)) in which Microsoft's Seattle Sidewalk site ([seattlesidewalk.com](#)) was linked to the Ticketmaster site in such a way as to by-pass its home page. It appeared that the ticketing process was being done on the Microsoft site whereas it was in fact delivered on the Ticketmaster site. One-nil to Ticketmaster.

The first major case using Intellectual Property to challenge framing, has settled. In [Washington Post Co. v. Total News](#), No. 97-1190 (S.D.N.Y.1997), Total News provided a web site that featured a list of "name-brand" news services, identified by their trademarks, in a narrow column to the left, an advertising banner across the bottom right of the screen, and a content window in the upper right of the screen. When a user clicked on a news service, that news service's content appeared within the content window on the Total News web site. However, when the news service's content first loaded, its advertisements were obscured by the advertising banner on the Total News web site. Some of the framed sites, such as CNN Interactive, responded by setting their pages to refresh when loaded so that the pages appeared in their own window without the Total News frame.

Although substantially a copyright case, the Total News plaintiffs (The Washington Post, Time, CNN, The Los Angeles Times, Dow Jones and Co., and Reuters) also alleged trademark infringement, false designation of origin, and unfair competition. On June 5, 1997, the parties settled with Total News agreeing to cease framing the plaintiffs' web sites in exchange for permission to link to the plaintiffs' web sites using hypertext reference links consisting only of highlighted plain text. Each plaintiff is entitled to revoke permission to link to its site; however, if the defendant refuses to remove the link the plaintiff must convince a court that the link is an impermissible violation of rights under some theory of intellectual property.

The Total News case demonstrates an important distinction between framing and linking in the context of advertising, the lifeblood of the web. With framing, the framing site's revenue generating advertisements are substantially more visible to the consumer than those of the framed site. Unlike the Total News style framing model, the hypertext reference linking model, permitted under the terms of the settlement, does not obscure the advertisements of the linked-to page. Where sites are linked, rather than framed, the link can enhance the revenues of both sites, providing additional consumers through links. Such economic benefits of linking, as well as the fair use nature of many such links, have led linking to be ubiquitous on the net.

Similarly, in the Shetland News Case (see [www.shetland-times.co.uk/st/ internet/legal.htm](#)), the defendant

company was framing content on the plaintiff's site. Again, users would not know that they were in fact viewing the site of the plaintiff. The deleterious effect on the value of the plaintiff's asset was inescapable.

What these brief allusions indicate is that the courts are applying the traditional concepts of Trade Practices and Intellectual Property and are providing protection for those who have invested in the development of the asset and have a reasonable business expectation to control the benefit of that asset.

METATAGGING/STUFFING

The final Internet technology affecting trademark that I wish to cover in this paper, is the process known as metatagging or stuffing. This is where one hides search words in the text so as to divert traffic to your site.

For example, in Playboy Enterprises Inc. v. Calvin Designer Label, Calvin Fuller and Calvin Merit, No. 97-3024 CAL (N.D. Cal. filed August 1997), the defendants, whose site also featured pornographic material, repeated the words PLAYBOY, PLAYBOY MAGAZINE AND PLAYMATE on their website several hundred times. The words were typed in black on a black background, so that although the user was oblivious to their presence, their search engines kept returning the defendant's site. Playboy Enterprises Inc. sued for, inter alia, trademark infringement, dilution and unfair competition, and while the case is still pending, it seems relatively straightforward, as a blatant misappropriation of corporate intellectual property.

I do not believe that the Australian courts will find such cases very difficult where they involve the appropriation of a mark owned by another. It is only worth metatagging a famous mark because only such a mark is likely to be input by web surfers. The more famous the mark, the more useful to the metatagger - but the more easy it is to win the subsequent trademark case.

Essentially, "stuffing" gets press because it is a new trick for the business world but the legal consequences will prove fairly banal.

To some extent such cases involving new technologies show the ability of our current legal paradigms to adapt to the challenges of these technologies.

PART B

COMPONENT / APPLICATION AUTHORSHIP

I want to end the paper with something a little lighter: the copyright consequences of the creation of new material

by application driven processes without human intercession.

Take a program which creates new musical works without the intervention, labour, judgment and skill of a living composer. This is the intriguing puzzle posed by an English gentleman who has developed a program which analyses, reassembles, edits and reformats the original works of JS Bach and from these components creates new musical works.

Who is the author of these new works for copyright purposes?

Is that authorship of a quality sufficient to bring the author within the "qualified person" test provided by s32 of the Copyright Act?

The Act does not help us further. It provides no definition of "author". But it requires that there is one.

So, who is the author of the new, albeit derivative, Bach-like work. Clearly the fact that the underlying works were written by a human composer cannot be relevant to authorship of the new work. No analysis would permit a result, which accorded Bach the authorship of the new work.

There are perhaps three possibilities:

- (i) The author of that new work is the person who presses the button, which activates the application;

This is unattractive. It is difficult to suggest that there is a sufficient degree of skill and labour required in the action of button pressing to amount to an act of authorship. That said, button pressing has become a core part of the electronic creator's skills but there is no statute or case law which tries to define the degree of skill and labour required.

The degree of skill and labour required must always be a question determined subjectively but in this case, I have little doubt that the mere pressing of an icon marked "Compose Now" would be insufficient to amount to an act of authorship. The analogy to the "mere amanuensis" in literary works, is obvious. It is not, in itself, an action worthy of attracting copyright.

- (ii) The author of that new work is the author of the software application;

This possibility is not as absurd as it sounds. The software application embodies everything necessary to create the new work: namely, all of the underlying works and the software program which undertakes all of the necessary processing. All that is required is a dumb act.

That said, without that dumb act the work remains inchoate. It would never exist except for that intervention. It would never receive a material form. It could never be a work at all. This takes us back to the suggestion that it is the icon presser who has given material form to the work and therefore should be accorded copyright - but we have already dismissed this possibility on other grounds!

(iii) There is no author for copyright purposes.

As difficult as this may be to accept, this may be the answer. The other possibilities have difficulties passing the various tests either of authorship or of the prerequisites for the subsistence of copyright. We must recognise the possibility that the new technologies have created the possibilities of creating musical compositions, which do not attract copyright.

For those who have a commercial reason to avoid this situation, the answers are clear enough: one lies in the design of the application and the other in contract. Which option is appropriate will depend on the result that the application vendor wishes to achieve:

- (a) if the intention is to permit the user of the application to be able to be the owner of the rights in the new work, the design should build in a sufficient, albeit low, hurdle of skill and labour on the part of the user.
- (b) If the application developer wishes to retain the rights in the material produced, it could do so by making it a condition of the licence that the user was acting as the agent or the developer for the purpose of giving the otherwise inchoate, a material form. It would pose an interesting challenge to those charged with the drafting of the "shrink-wrap" or "web-wrap" licence agreements!

I have used the example of the new Bach because it is more fascinating than the usual discussions about who owns the rights in databases created by automated, software-driven applications. Database creation was one of the first and obvious uses of software driven, non-author driven applications. The commercial value of copyright starts with an ability to own it, to treat it as property. Information Technology is going to increasingly challenge our ability to determine the ownership of that property by the application of traditional copyright principles.

CONCLUSION

The law, which has evolved to regulate the protection of name and reputation in the atom-based business community, has coped very well with business' move into cyber-commerce. We would expect nothing less of it!

However, while it is readily conceded that many of the problems identified in this paper are, in essence, not new, I would suggest that there is sufficient novelty in cyberspace to warrant a legislative effort aimed specifically at addressing these new circumstances.

I do not wish to engage in the reform issues today. That is a topic of its own and deserves very detailed consideration - not just of local laws and local issues but also of the international ramifications of any such initiatives.

For example, can we afford to have a domain name registration system that is outside government control? Should government be laying down rules for the orderly allocation of names and the resolution of disputes? Should we not already be reviewing the existing legislation to see how it can better provide for the needs of e-commerce?

Quite simply, the need for review and reform, like the technology which drives it, is constant.