

Internet Domain Name Dispute Resolution

David Lindsay¹

Paper presented to BLEC Congress 2002

Melbourne, 30 April 2002

1. Introduction

Internet domain names are resources that have come to perform a number of important economic and social functions. The use of domain names has given rise to novel legal and commercial issues and has led to the development of new legal and quasi-legal structures and rules. There have been two main areas of legal controversy:

- The development of appropriate institutional arrangements concerning policy-making, rule-making and management of Internet domain names (generally known as domain name ‘governance’ issues); and
- The relationship between domain names and existing intellectual property rights (IPRs), especially trade marks.

This paper deals only briefly with the complex issues relating to international domain name governance. The focus of the paper is on the development of legal principles for resolving conflicts between conventional IPRs, especially trade marks, and domain names. Specifically, it concentrates on two main issues. First, the paper explains the circumstances in which the registration or use of a domain name is likely to result in an infringement of an IPR, such as a trade mark, under Australian law. Second, the paper deals with domain name dispute resolution procedures and, in particular, with the international mandatory administrative procedure known as the Uniform Dispute Resolution Procedure (UDRP). It explains the origins of the UDRP and the way the UDRP has been interpreted in practice. It further deals with judicial challenges to the UDRP and dispute resolution in the .au namespace. The paper concludes with some observations regarding the developing law in relation to Internet domain names.

2. The Domain Name System

The Domain Name System (DNS) is a distributed, hierarchical database of Internet name and address information. The purpose of the DNS is to resolve, or map, the names of host computers to numerical IP (Internet Protocol) addresses. Every computer connected to the Internet has its own unique IP address. The IP address is a 32-bit number that is conventionally presented in dotted decimal form divided into four binary octets.²

¹ Research Fellow, Centre for Media, Communications and IT Law, The University of Melbourne. E-mail: dlindsay@unimelb.edu.au.

² See Paul Mockapetris, ‘Domain Names – Concepts and Facilities’, RFC 1034, November 1987 available at <http://www.ietf.org/rfc/>.

The domain name is an alphanumerical name that corresponds to the IP address. The founders of the Internet introduced the concept of domain names because alphanumerical names are easier for humans to understand and remember than relatively long, meaningless IP addresses. For example, the IP address for the Faculty of Law at the University of Melbourne is 128.250.165.111. While computers have no difficulty in processing the binary information that constitutes an IP address, it is much easier for humans to deal with the address in alphanumeric form, namely <law.unimelb.edu.au>.

3. Domain Names

The domain name space is organised hierarchically according to a root and tree structure. When read from left to right, the name follows a path from the branches of the tree to the root. A domain name, such as <law.unimelb.edu.au>, essentially consists of three main elements: the top-level domain (TLD), second-level domain (2LD) and third or higher-level domains.³

There are two groups of top-level domains, generic TLDs (gTLDs) and country code TLDs (ccTLDs). In 1983, Jon Postel and Joyce Reynolds defined the following six original gTLDs.⁴

GTLTD	Purpose
.com	commercial
.edu	education
.gov	government
.mil	military
.net	network resources
.org	other organisations

The .com, .net and .org gTLDs are known as open gTLDs, as there are no restrictions on eligibility for registration. The .edu, .gov and .mil gTLDs are known as closed gTLDs, as registrations are confined to educational institutions, United States federal government organisations and United States military organisations, respectively. A .int gTLD was later added for international organisations.⁵ In November 2000, the following seven new gTLDs were approved:

GTLTD	Purpose
.aero	air transport industry
.biz	business or commercial purposes
.info	information
.coop	cooperatives

³ As Sumption QC (sitting as a Deputy Judge of the High Court) put it in *Marks & Spencer v One in a Million* (1997) 42 IPR 309 at 310: 'A domain name comprises groups of alphanumeric characters separated by dots'.

⁴ Jon Postel and Joyce Reynolds, 'Domain Requirements 1', RFC 920, available at <http://www.ietf.org/rfc/>.

⁵ There is also one four-letter gTLD, the .arpa gTLD, which is used for reverse IP lookups.

.museum	museums recognised by International Council of Museums (ICOM)
.name	individuals
.pro	professionals

The .info gTLD is an open gTLD, whereas the other new gTLDs are closed.

The second group of top-level domains are known as country code TLDs (ccTLDs). Country code TLDs consist of two-letter abbreviations of country names, such as .au for Australia, .fr for France, or .tv for Tuvalu. Almost all of the ccTLDs are derived from the International Organization for Standardization’s ISO Standard 3166.⁶ The requirements for registration of domain names under ccTLDs differ considerably, depending upon the policies of authorities responsible for the ccTLD. For example, there are almost no rules applying to registrations under the .tv ccTLD, but quite a number of rules applying to registration under the .au ccTLD.

The second part of a domain name is known as a second-level domain, or 2LD. For example, in the domain name, <law.harvard.edu>, the gTLD is .edu and the 2LD is .harvard.edu. By way of contrast, in the domain name <law.unimelb.edu.au>, the ccTLD is .au and the 2LD is .edu.au. The 2LDs under the .au ccTLD include: .com.au, .edu.au, .gov.au, .net.au and .org.au. Some domain names have only two elements, a TLD and a 2LD. Where a domain name consists of more than two domains, the remaining elements are known as third or higher-level domains. Thus, in the domain name <law.harvard.edu> ‘.law’ is a third level domain, whereas in the domain name <law.unimelb.edu.au>, ‘law.unimelb’ are third or higher-level domains.

4. ICANN and DNS Governance

In the late 1990s, the popularity and commercialisation of the Internet resulted in pressures to reform the management of the DNS. DNS administrative and management functions had originally been performed relatively informally, and largely on a voluntary basis. In June 1998, the United States Department of Commerce published a policy statement proposing the creation of a new private, non-profit corporation to perform DNS management functions, including overseeing policy for adding new TLDs.⁷ The Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organisation incorporated under Californian law, was established as a result.

The legal arrangements relating to the establishment of ICANN are complex. The most important founding documents consist of a set of interlocking contracts between the United States Department of Commerce (DoC), ICANN and a private company, Network

⁶ ISO 3166-1: *Codes for the Representation of Names of Countries and Their Subdivisions – Part 1*, available at http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html.

⁷ National Telecommunications and Information Administration (NTIA), *Management of Internet Names and Addresses*, 63 Fed Reg 31,741 (June 1998) (commonly known as the *Magaziner Report* or *White Paper*).

Solutions, Inc (NSI), which was responsible for administering and maintaining the authoritative DNS root server. The agreements, which were finalised in November 1999, had a number of important consequences. First, the agreement between the DoC and ICANN ensured that the United States government preserves a residual degree of policy supervision over ICANN.⁸ Second, the agreement between DoC and NSI ensured that domain name registrations would be accepted only from ICANN-accredited registrars.⁹ This effectively meant that ICANN could impose conditions, through accredited registrars, on all domain name registrants. Third, under the registry agreement between ICANN and NSI, NSI agreed to require all registrars to adopt a dispute resolution policy to be enforced on all domain name registrants.¹⁰

Since its inception, the legitimacy of ICANN has been questioned.¹¹ There are three main question-marks over ICANN's legitimacy. First, none of the parties to the 1999 agreements could claim unequivocal authority over the DNS and the DNS legacy root. Second, the agreements did not clarify ultimate responsibility for DNS policy-making, and ICANN has sought to maintain the fiction that its role is confined to technical coordination, not policy-making. Third, and perhaps most importantly, mechanisms for ensuring the legal accountability of ICANN were, at best, ambiguous. In particular, the full extent to which ICANN is accountable to the United States government, or to an amorphous 'Internet community', is unclear. Moreover, as a private organisation, ICANN is not subject to legal mechanisms that have been developed to ensure accountability of public policy-making bodies.

Given the inadequate institutional foundations of ICANN, it is unsurprising that most stakeholders and commentators have come to regard the current arrangements as unsustainable. The focus of policy debates has shifted from the legitimacy of the existing structure to proposals for restructuring or replacing ICANN. In February, the President of ICANN, Stuart Lynn, released a report, entitled *ICANN – The Case for Reform*, designed to stimulate public discussion of the future of arrangements for managing the DNS.¹² In essence, the report advocated a greater role for national governments within ICANN, including representation at the board level. It also recommended new mechanisms to increase the transparency and accountability of ICANN processes. Over

⁸ See *Memorandum of Understanding Between the US Department of Commerce and Internet Corporation for Assigned Name and Numbers, Amendment 1* (November 4, 1999), available at <http://www.icann.org/nsi/coopagmt-amend1-jpamou-04nov99.html>.

⁹ See *DoC-NSI Cooperative Agreement, Amendment 19* (November 4, 1999), available at <http://www.icann.org/nsi/coopagmt-amend19-04nov99.html>.

¹⁰ See *ICANN-NSI Registry Agreement* (November 4, 1999), available at <http://www.icann.org/nsi/nsi-registry-agreement-04nov99.html>.

¹¹ See, for example, A Michael Froomkin, 'Wrong Turn in Cyberspace' (2000) 50 *Duke Law Review* 17; Jonathan Weinberg, 'ICANN and the Problem of Legitimacy' (2000) 50 *Duke Law Review* 187; Milton Mueller, 'ICANN and Internet Governance' (1999) 1(6) *Info* 497; David Lindsay, 'Should We Believe in Rough Consensus? ICANN and the Problem of Legitimacy in Managing the Domain Name System (DNS)' Paper presented to Communications Research Forum, Canberra, 27 September 2001, available at <http://www.dcita.gov.au/crf/>.

¹² Stuart Lynn, *ICANN – The Case for Reform*, February 2002, available at <http://www.icann.org>.

time, it is likely that arrangements for managing the DNS will benefit from more formal structures of accountability and a formally recognised role for national governments.¹³

5. The Problem of ‘Cybersquatting’

The DNS was designed by non-lawyers and developed before the Internet began to be used commercially. The founders of the Internet were predominantly concerned with technical matters, not with potential legal conflicts. When the DNS was established, there was no way of predicting the difficulties that would arise from conflicts between Internet identifiers and real-world identifiers, such as trade marks.

From the mid-1990s, the growing commercialisation of the Internet was associated with a change in the functions of domain names. Because domain names were designed to be easily remembered, they began to be used by businesses as a means of identifying themselves and their products. Since then, domain names rapidly developed into an accepted form of identification not only in the on-line environment, but off-line as well. Difficulties arose, however, largely because registration in the original open TLDs - .com, .net and .org – was on a ‘first-come, first-served’ basis, with no vetting of applications. In other words, there was no need for an applicant to establish any association with a domain name in order to be registered as the domain holder.

The practice known as ‘cybersquatting’ was the predictable outcome of the increase in the commercial value of domain names together with the policy of granting a domain name to the first applicant to pay a fee. This created an incentive for an applicant to register a domain name with the intention of selling it to those with an interest in the real world identifier - such as a trade mark or famous name – corresponding to the domain name. Cybersquatting was initially able to succeed because of the low costs of registering a domain name when compared with the commercial value of real-world identifiers, such as trade marks. As a result of the high costs of defending a real-world identifier, those with an interest in the identifier, such as a trade mark owner, had an incentive to pay cybersquatters to obtain the domain name, rather than to commence legal proceedings. Furthermore, there was considerable legal uncertainty in relation to whether registration of a domain name that corresponded to a trade mark would amount to trade mark infringement. Trade mark owners also became concerned with other practices, such as the registration of domain names in order to unfairly trade off the business reputation of a trade mark owner.

6. Differences between Domain Names and Trade Marks

To an extent, a degree of conflict between domain names and trade marks is inevitable. This is because domain names differ from real-world identifiers, such as trade marks, in some important respects.

¹³ See Lindsay (2001) *supra*.

First, domain names and trade marks perform different functions. Domain names, like the IP addresses to which they correspond, serve to identify the position of a host computer in a logical space, the Internet. In addition to mapping to IP numbers, however, domain names may also assist in locating an Internet site. For example, a person interested in finding a site relating to coca cola may enter the url <cocacola.com> and be directed to the appropriate site. In other words, domain names can perform a directory-like function. Finally, with the commercialisation of the Internet, domain names have become associated with real-world entities, sometimes performing a trade mark-like function of identifying the source of goods or services. A trade mark, on the other hand, performs one main function: identifying the origin of a product.¹⁴ By communicating information to consumers concerning the source of a product, a trade mark serves to provide consumers with information about a product that would otherwise be unobservable. This facilitates the operation of markets by creating an incentive for firms to produce products with features that consumers wish to purchase.¹⁵ Beyond this traditional function of trade marks, especially well-known marks may have an intrinsic commercial value, that may then be used for other commercial purposes, such as being attached to other products that the firm produces.¹⁶ The registration and use of a trade mark as a domain name by an entity other than the trade mark owner may create confusion about the use of the trade mark, thus interfering with the function of the trade mark as a ‘badge of origin’ of a product. The use of a trade mark as a domain name may also dilute the intrinsic value of a well-known mark.

Second, as a result of the technical requirements of the DNS, each domain name, much like a telephone number, is necessarily unique.¹⁷ Trade marks, on the other hand, are not necessarily unique; different firms may have rights to the same trade mark. As trade marks are registered in respect of particular classes of goods or services,¹⁸ provided there is no likelihood of confusion, the same trade mark may be registered by different owners in relation to different goods or services.¹⁹ Furthermore, as a mark may be known only in a certain geographical area, the same trade mark may be registered by different owners in relation to different geographical areas. Given the unique nature of a domain name, it is

¹⁴ As Bowen LJ stated in *Powell’s Trade Mark*: ‘The function of a trade mark is to give an indication to the purchaser or possible purchaser as to the manufacture or quality of the goods, to give an indication to his eye of the trade source from which the goods came, or the trade hands through which they pass on their way to the market’: (1893) 10 RPC 195 at 200. See also: *Aristoc Ltd v Rysta Ltd* (1945) 62 RPC 65; *Shell Co of Australia Ltd v Esso Standard Oil (Aust) Ltd* (1963) 109 CLR 407.

¹⁵ See Nicholas Economides, ‘Trademarks’ in *New Palgrave Dictionary of Economics* (December 1997), available at <http://raven.stern.nyu.edu/networks/>.

¹⁶ The High Court has pointed out that this intrinsic value has come to be protected by actions against trade mark dilution: *Campomar v Nike International* (2000) 202 CLR 45.

¹⁷ Leaving aside the issue of alternative root directories.

¹⁸ *Trade Marks Act 1955* (Cth) s 19.

¹⁹ In *Southern Cross Refrigerating Co v Toowomba Foundry Pty Ltd* (1954) 91 CLR 592, it was held that confusion would be likely if the goods were likely to be dealt with in the same kind of market and bought by the same type of purchaser. Furthermore, there may be a likelihood of confusion if goods or services are associated in some way because of some trade connection: see, for example, *Sym Choon & Co Ltd v Gordon Choons Nuts Ltd* (1949) 80 CLR 65; *HJ Lees & Sons (London) Ltd’s Application* (1955) 72 RPC 75.

clear that all those with a legitimate interest in a trade mark cannot possibly have rights in relation to a domain name that includes the trade mark.

Third, a trade mark is a form of property, but it seems that, at least for most present purposes, a domain name is not. Section 21 of the *Trade Marks Act 1955* (Cth) expressly provides that a registered trade mark is a form of personal property. The question of whether a domain name is a form of property has yet to come before the courts in either Australia or the United Kingdom. The issue has, nevertheless, been the subject of a number of decisions by courts in the United States. To date, United States courts have held that registration of a domain name gives rise to contractual rights, not property rights. The issue has come before United States courts in a number of contexts. For example, in *Network Solutions, Inc v Umbro International Inc*,²⁰ Umbro obtained a default judgment against a Canadian company for registering <umbro.com>, and sought to enforce it by garnisheeing the assets of the Canadian company held in the United States. The only assets the Canadian company held in the United States were 38 domain names registered with Network Solutions. Umbro could only succeed against Network Solutions if the domain names were a form of property. The majority of the Supreme Court of Virginia held that registration of a domain name is a contract for services giving rise to a contractual right to use a domain name and, therefore, the domain names were not subject to garnishment. In reaching this decision, the court drew analogies between the registration of a domain name and a subscription fee paid by a satellite television subscriber, and with registration of a business name.

In *Kremen v Stephen Michael Cohen*,²¹ the plaintiff, Kremen, registered the domain name <sex.com> in 1994. The name was subsequently transferred to Cohen as a result of a letter sent to the registrar, Network Solutions. Kremen maintained that the letter was a forgery. He sued Network Solutions alleging a number of causes of action, including breach of contract, conspiracy to commit conversion and breach of a bailor/bailee relationship. A Californian federal District Court held that a domain name was not a form of tangible property and was not a form of intangible property entitled to protection by an action for conversion. The court held that extending property rights to domain names was properly a matter for the legislature, not the courts. The court also held that Network Solutions was not a bailee, as its role was merely to provide the service of registering domain names. The decision is currently on appeal before the 9th US Circuit Court of Appeals.

In the most recent United States decision, *Zurakov v Register.com*,²² Zurakov entered an agreement with the registrar, Register.com, to register the domain name <laborzionist.com>. Prior to construction of the site, Register.com linked the home page to their own 'Coming Soon Page', which contained banner advertisements. Zurakov objected to this use of the home page. Amongst other things, Zurakov argued that he had an exclusive property right in the domain name that was interfered by Register.com's use of the home page. The Supreme Court of New York essentially followed *Umbro* in

²⁰ 529 SE 2d 80 (1999).

²¹ 99 F Supp 2d 1168 (2000).

²² Supreme Court of the State of New York, case no 600703/01, 25 September 2001.

concluding that Zurakov had a contractual right and not a property right in the domain name. The court held that the service agreement exclusively governed Zurakov's rights to use the domain name and dismissed the complaint.

The position in the United States is somewhat complicated by legislation known as the *Anticybersquatting Consumer Protection Act* (the *ACPA*),²³ which is dealt with further below. This legislation provides that domain names may be subject to *in rem* actions, which are available only in relation to property. This provision was introduced to allow a trade mark owner to initiate proceedings under the *ACPA* against the domain name itself where the registrant either cannot be located, or is not amenable to personal jurisdiction. An *in rem* action is available only if the plaintiff can establish that the court was not able to obtain *in personam* jurisdiction over the defendant or that, through due diligence, it was not possible to find the defendant. The remedies available in respect of *in rem* actions are limited to cancellation of the domain name, or transfer of the domain name to the plaintiff.

7. Cybersquatting, Trade Mark Law and Passing Off

To date, Australian courts have not given detailed consideration to the issue of whether the registration or use of a domain name amounts to a trade mark infringement, or gives rise to an action for passing off. To some extent, we must therefore rely on decisions from comparable jurisdictions.

7.1 UK Cases

For the purposes of the law of passing off, the most significant English precedent is the 1998 decision of the Court of Appeal in *British Telecommunications Plc v One in a Million Ltd.*²⁴ In that case, One in a Million, and associated companies, engaged in the business of registering well known names, such as British Telecom and Marks & Spencer, as domain names, without the consent of the firms that owned the goodwill in the names. The domain names were not actively used by One in a Million, but were registered with the intention of selling the names to the firms who owned goodwill in the names, to block registration, or to sell the names to other firms. At first instance, Sumption QC held that, although mere registration of a 'deceptive' domain name did not amount to a passing off, an injunction would be awarded to restrain a threatened passing off. He held that there would be a threat of passing off in the future if registration of a domain name was calculated to infringe the rights of the owner of the goodwill in the name. In finding that there was a threatened passing off, he concluded that:

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

²³ 15 USCA s 1125(d).

²⁴ (1998) 42 IPR 289.

restrain the threat of passing off, and the injunction will be in terms which will make the name commercially useless to the dealer.²⁵

Sumption QC also found that the activities of One in a Million constituted a trade mark infringement under section 10(3) of the *Trade Marks Act 1994* (UK).

The Court of Appeal upheld the first instance decision in relation to both passing off and trade mark infringement, but with some important differences in reasoning. The court granted an injunction to prevent passing off on two bases. First, unlike the first instance decision, the court held that mere registration of a ‘deceptive’ name constituted a passing off. To maintain an action for passing off a plaintiff must generally establish the following three elements:

- A reputation or goodwill in an indicia deserving protection;
- Misrepresentation likely to confuse or mislead the relevant public; and
- Damage, or likelihood of damage, suffered as a result of the misrepresentation.²⁶

The court held that registering a distinctive mark, such as Marks & Spencer, amounted to a misrepresentation that the domain name registrant was connected or associated with the owner of the goodwill in the name.²⁷ The misrepresentation would be conveyed to anyone who became aware of the identity of the domain name registrant by, for example, accessing the ‘whois’ database. Moreover, the court held that the misrepresentation diminished the exclusive goodwill in the name, resulting in damage or the likelihood of damage, to the owner of the goodwill. Second, the court held that an injunction would be available in a passing off case where the defendant either equips himself or herself with, or intends to equip another with, an ‘instrument of fraud’.²⁸ The court essentially held that a domain name consisting of a well-known name was an instrument of fraud. It concluded that:

The registrations were made with the purpose of appropriating the respondents’ property, their goodwill, and with an intention of threatening dishonest use by them or another. The registrations were instruments of fraud and injunctive relief was appropriate just as much as it was in those cases where persons registered company names for a similar purpose.²⁹

The Court of Appeal confirmed that registration of the domain names was a trade mark infringement under United Kingdom trade marks law, as registration was for the purpose of selling domain names that were confusingly similar to registered trade marks. Given

²⁵ (1997) 42 IPR 309 at 314.

²⁶ See *Fletcher Challenge Ltd v Fletcher Challenge Pty Ltd* [1981] 1 NSWLR 196; *Reckitt & Colman Products Ltd v Borden Inc* (1990) 17 IPR 1; *Consorzio del Prosciutto di Parma v Marks & Spencer plc* [1991] RPC 351.

²⁷ (1998) 42 IPR 289 at 305.

²⁸ (1998) 42 IPR 289 at 302. Aldous LJ held that a domain name would be an instrument of fraud if it was registered by the defendant with the intention of appropriating the goodwill of another.

²⁹ (1998) 42 IPR 289 at 307.

the differences between United Kingdom trade mark law and Australian law, however, the court's conclusions on the trade mark issue are of only limited relevance in Australia.

Although the reasoning in *One in a Million* has been accepted in subsequent United Kingdom decisions,³⁰ registration of a domain name that contains a registered trade mark clearly does not invariably constitute trade mark infringement under United Kingdom law. For example, in *Avnet Inc v Isoact Ltd*,³¹ the plaintiff was the owner of the trade mark 'AVNET', which was registered in relation to advertising and promotional services. The plaintiff sold technical goods by means of a catalogue and an associated Web page. The defendants provided Internet services, especially to the aviation industry, including hosting Web pages. As part of their business, the defendants owned the domain name <avnet.co.uk> and provided a service for customers to display their own advertisements. The plaintiff contended that use of the word 'avnet' on the Internet amounted to an infringement of the 'AVNET' trade mark. Laddie J held that, although the defendant was providing a facility for their customers to advertise, it did not provide advertising and promotional services. As the defendant did not use the word 'avnet' in relation to the class of services for which the trade mark was registered, there was no trade mark infringement.

7.2 Australian law

In *One in a Million*, the English Court of Appeal referred to a number of cases in which registration of a company name resembling the trading name of a corporation was held to amount to passing off.³² As Aldous LJ pointed out, cases where a company name is registered in order to trade off the goodwill of another firm are analogous to cases involving the registration of a domain name. Provided that a plaintiff firm can establish a reputation in the name, difficulties may arise in relation to whether mere registration of the name as a domain name amounts to a misrepresentation such as to damage the goodwill of the plaintiff. It was largely to surmount these difficulties that the court interpreted cases involving registration of a company name as establishing an independent form of liability for passing off where a defendant equips himself or herself, or intends to equip another, with an 'instrument of fraud'.

The main Australian authority dealing with whether registration of a company name is a passing off is *Fletcher Challenge Ltd v Fletcher Challenge Pty Ltd*.³³ In that case, shortly following the incorporation of Fletcher Challenge Ltd in New Zealand, the defendants applied for the reservation of the company name 'Fletcher Challenge Pty Ltd' in New South Wales, and later incorporated a shelf company of the same name. After concluding that the New Zealand company had sufficient reputation in New South Wales, Powell J held that if the defendant were to commence trading they would be associated

³⁰ See, for example, *easyJet Airline Co Ltd v Dainty t/as easyRealestate* [2002] FSR 6.

³¹ [1998] FSR 16.

³² *Panhard et Levasser v Panhard Levasser Motor Co Ltd* [1901] 2 Ch 513; *Suhner & Co AG v Suhner Ltd* [1967] RPC 336; *Fletcher Challenge Ltd v Fletcher Challenge Pty Ltd* [1982] FSR 1; *Direct Line Group Ltd v Direct Line Estate Agency Ltd* [1997] FSR 374; *Glaxo Plc v Glaxowellcome Ltd* [1996] FSR 388.

³³ [1981] 1 NSWLR 196.

with the plaintiffs in the minds of the relevant public. He further held that the misrepresentation of an association would be likely to damage the reputation of the plaintiffs.³⁴ Thus, the mere registration of a company name may be sufficient to constitute a passing off provided that there is a misrepresentation of an association with another entity that has a reputation in the name, even if the defendant does not use the name in connection with trading activities.³⁵ By analogy, registration of a domain name may amount to a passing off if the registration involves a misrepresentation of an association with a company that has goodwill in the name. As yet, it would seem premature to conclude that there is an independent basis of liability in passing off under Australian law where a defendant is equipped with an instrument of fraud, such as a registered domain name, as suggested in *One in a Million*.

Whatever the position under English law following the *One in a Million* decision, it seems clear that, under Australian law, an action for passing off cannot be made out if there is no misrepresentation.³⁶ Two Federal Court decisions have considered the circumstances in which registration of a domain name will not amount to a misrepresentation. Both cases were concerned with allegations of misleading or deceptive conduct in breach of section 52 of the *Trade Practices Act 1974* (Cth), not with the tort of passing off. For most purposes, however, the principles applied in determining whether there is a breach of section 52 will be the same as those applied in cases dealing with passing off.³⁷

In *Capital Webworks Pty Ltd v Adultshop.Com Ltd*,³⁸ the applicant company had registered the domain name <adultshop.com.au> for use in retailing adult leisure products. As a result of an error, registration of the domain name was not renewed. Following the lapse in registration the domain name was allocated to the respondent company, adultshop.com. The applicant alleged that use of the domain name was misleading and deceptive in breach of section 52. Nicholson J, however, held that there was no misrepresentation resulting from the use of the domain name by the respondent. In particular, as users of the <adultshop.com.au> Web site were directed to the site operated by adultshop.com, there was no misrepresentation of an association between the respondent and the applicant, Capital Webworks. Nicholson J also doubted whether Capital Webworks had any goodwill in the domain name.

³⁴ Powell J found an alternative basis for liability in the law of civil conspiracy.

³⁵ In *One in a Million* Aldous LJ maintained that Powell J ‘must have concluded that the name of the company was an instrument of fraud as its use would mean that passing off would result’: (1998) 42 IPR 289 at 301. There is absolutely nothing in the *Fletcher Challenge* decision to substantiate this interpretation.

³⁶ As Gummow J pointed out in *ConAgra Inc v McCain Foods (Aust) Pty Ltd* (1992) 33 FCR 302 at 365: ‘... misrepresentation is the gist of the action’.

³⁷ For some differences between the tort of passing off and section 52 see, for example, *Peter Isaacson Publications Pty Ltd v Nationwide News Pty Ltd* (1984) 56 ALR 495. In that case it was established that an action for breach of section 52 could be sustained even though there was insufficient reputation to maintain a passing off action.

³⁸ [2000] FCA 492 (5 April 2000).

The issue of whether registration and use of similar domain names is likely to be misleading arose recently in *Sydney Markets Ltd v Sydney Flower Market Pty Ltd*.³⁹ The case concerned a dispute over the commercial use of the words ‘Sydney Flower Market’. The applicant alleged that use of the words by the respondent was a contravention of section 52, and the respondent counter-claimed. Hely J concluded that, largely because the parties conducted non-competing businesses in different markets, there was an honest concurrent use of the name. The main claim was, accordingly, dismissed. The use of similar domain names was, nevertheless, dealt with separately. The possibility for confusion arose from the registration of competing domain names. The respondent registered the domain name <sydneyflowermarket.com.au> in mid-1998 and thereafter used the site to market flowers on-line. The applicant subsequently registered the domain name <sydneyflower.com.au> and, after a period of time, registered the domain names <sydneyflowermarket.com>, <sydneyflowermarket.net> and <sydneyflowermarket.net.au>. Hely J held that use of the similar domain names was likely to mislead the public, stating that:

... where two domain names are sufficiently similar so as to make it difficult for a member of the public to know in advance exactly which site they will be taken to (as, for example, where the only difference between them is the presence or absence of “.au”), there is considerable scope for the public to be misled ... There is some evidence that a person seeking to access the respondent’s site kept arriving at the applicant’s site, presumably by reason of the failure to enter the “.au”, which alone serves to distinguish between the addresses of the two sites. The similarity between the website addresses is such that those members of the public who wish to order flowers from the respondent by means of the Internet, might by mistake access one of the applicant’s sites, and persons seeking the applicant’s site may arrive at that of the respondent.⁴⁰

Although Hely J held that concurrent use of the domain names would breach section 52, he found that the use would not be misleading if appropriate disclosures or disclaimers were put on the Web sites. In most circumstances, the courts have been reluctant to conclude that disclaimers have the effect of negating a misrepresentation. For example, in *Hutchence v South Seas Bubble Co Pty Ltd*, Wilcox J stated that:

There are occasions upon which the effect of otherwise misleading or deceptive conduct may be neutralised by an appropriate disclaimer ... But such cases are likely to be comparatively rare and to be confined to situations in which the court is able to reach satisfaction – the onus resting on the party relying on the disclaimer – that the disclaimer is likely to be seen and understood by all those – leaving aside isolated exceptions – who would otherwise be misled before they act in relation to the relevant transaction.⁴¹

³⁹ [2002] FCA 124 (22 February 2002).

⁴⁰ [2002] FCA 124 at paras 149-150.

⁴¹ (1986) 6 IPR 473 at 481.

Hely J, however, granted cross-injunctions, ordering the parties to post appropriate disclaimers on the Web sites. In doing so, he maintained that: ‘(w)ilst disclaimers (particularly on the labels for products) are often regarded as insufficient to avoid the public being misled, the same considerations are not applicable in the case of a website’.⁴² Hely J was seemingly prepared to give greater weight to disclaimers included on Web sites than to other forms of disclaimer, such as labels, because those accessing the site might be more likely to read the disclaimer. Another relevant consideration would seem to be the apparent need for similar domain names registered to different owners to co-exist. In any case, much may depend upon the form of the disclaimer, including its relative prominence and whether a hyperlink is provided to the potentially misleading site. Moreover, a disclaimer may not be sufficient to remove liability in conventional cases of cybersquatting, where a domain name is registered with the intention of transferring it to a person with an interest in a similar real world identifier, or to a third party.

The issue of whether the registration or use of a domain name may constitute a trade mark infringement has yet to come before the courts in Australia. Nevertheless, in appropriate circumstances, registration or use of a domain name is likely to amount to an infringement of a registered trade mark under section 120 of the *Trade Marks Act 1995* (Cth). Different considerations apply depending upon whether or not the trade mark is well known in Australia.

First, to constitute an infringement under section 120(1), the trade mark owner must establish that the domain name:

- is used as a trade mark;
- is used in relation to registered goods or services ‘in the course of trade’;⁴³ and
- is substantially identical or deceptively similar to the registered trade mark.

Use of an identifier as a trade mark must be a use that distinguishes goods or services from the goods or services dealt with or provided by others.⁴⁴ As explained above, domain names have come to perform a number of functions, including identifying the source of goods or services. Consequently, if it can be established that the domain name is functioning as a badge of origin, then the first element of section 120(1) may be made out. Where a domain name is not being used, but is merely being passively held, there are obvious difficulties in establishing the second element. Nevertheless, in the *One in a Million* case, the English courts held that use in the course of a business of dealing in

⁴² [2002] FCA 124 at para 152.

⁴³ Section 120(1) does not expressly provide that it is necessary to establish that the mark has been used ‘in the course of trade’ to make out an infringement under the section. Nevertheless, the requirement remains relevant as section 17 defines a ‘trade mark’ as a sign used to distinguish goods or services dealt with, or provided ‘in the course of trade’. Use of a trade mark ‘in the course of trade’ essentially means that some commercial advantage has been obtained from the goodwill derived from the registered trade mark: *Shell Co of Australia v Esso Standard Oil (Australia) Ltd* (1963) 109 CLR 407.

⁴⁴ See the definition of a ‘trade mark’ in section 17 of the *Trade Marks Act 1995* (Cth).

domain names could amount to use of the trade mark in the course of trade.⁴⁵ Australian courts may well adopt a similarly flexible approach. In determining whether an identifier, such as a domain name, is deceptively similar to a registered trade mark, regard must be had to section 10 of the *Trade Marks Act 1995* (Cth). Section 10 provides that a mark is deceptively similar if ‘it is likely to deceive or cause confusion’. Moreover, under section 120(2), there is no infringement of section 120(1) if it can be established that use of the identifier is not likely to deceive or cause confusion. It may be that, depending upon the circumstances, any confusion between a domain name and a registered trade mark may be dispelled by a user accessing the relevant Web site. On the other hand, especially given the meaning that domain names have acquired off-line, there may continue to be confusion among people who do not access the site. In any case, as is clear from the *Avnet* decision, there is unlikely to be confusion where a domain name is used in connection with different goods and services to that in relation to which the trade mark is registered.

Second, if it can be shown that a registered trade mark is well known in Australia, it is potentially easier to establish that registration or use of a domain name infringes the trade mark. Under section 120(3), a well known trade mark can be infringed by an identifier, such as a domain name, even if the identifier is used in connection with unrelated goods or services, meaning goods or services that are not of the same description of the registered goods or services, or that are not closely related to the registered goods or services. If a trade mark is well-known, it will be infringed under section 120(3) if:

- the identifier is substantially identical with, or deceptively similar to, the registered trade mark;
- the identifier is used as a trade mark in relation to unrelated goods or services;
- because the trade mark is well known, the identifier would be likely to be taken as indicating a connection between the unrelated goods or services and the registered trade mark owner; and
- for that reason, the interests of the registered owner are likely to be adversely affected.

This provision was enacted to ensure compliance with Australia’s obligations to protect well-known trade marks under the *TRIPs Agreement*.⁴⁶ It appears to reflect the extent to which well-known marks may acquire a value that is independent of the use of a mark in relation to particular goods or services. The High Court acknowledged this independent function of well-known marks in *obiter* comments in *Campomar v Nike International*, made in connection with section 120(3):

⁴⁵ Aldous LJ stated that the marks ‘will be used in relation to the services provided by the registrant who trades in domain names’: (1998) 42 IPR 289 at 307. See also the decision of the New Zealand High Court in *DB Breweries Ltd v The Domain Name Co Ltd* (Unreported, Randerson J, 15 March 2001, High Court of New Zealand).

⁴⁶ General Agreement on Tariffs and Trade (1994), *Agreement on Trade-Related Aspects of Intellectual Property Rights*, Articles 16(2) and (3).

Such provisions represent legislative responses to the claims of trade mark owners to protection where, particularly by successful advertising, the fame of a mark carries its function beyond the traditional role as an identifier of origin. The ‘dilution’ theory of liability ‘does not require proof of a likelihood of confusion’; rather, what is protected is ‘the commercial value or ‘selling power’ of a mark by prohibiting uses that dilute the distinctiveness of the mark or tarnish the associations evoked by the mark.’⁴⁷

It may be that these comments suggest that the likelihood of a connection being made between the unrelated goods or services and the trade mark may be considered more important than any likelihood of confusion resulting from a similarity in the identifiers. In any case, provided a registered trade mark is well-known, use of a similar domain name may contravene section 120(3), even if the name is not used in connection with goods or services in relation to which the trade mark is registered. As with passing off actions, the important consideration is whether registration or use of a domain name is likely to result in a connection being drawn with the registered trade mark owner.

8. The Uniform Dispute Resolution Policy (UDRP)

As explained above, as the Internet grew in popularity through the 1990s, conflicts between domain names and real world identifiers, such as trade marks, became inevitable. Such conflicts were exacerbated by the open slather ‘first-come-first-served’ registration policy for the three open gTLDs, .com, .org and .net. Given the difficulties and costs involved in bringing traditional court proceedings – including the difficulties of commencing proceedings against domain name registrants located outside the court’s jurisdiction and the uncertain application of conventional actions, such as trade mark infringement or actions under ‘unfair competition’ laws, including the Australian action for passing off – trade mark owners became interested in establishing a streamlined, inexpensive non-national dispute resolution system. This eventually led ICANN to adopt an informal dispute resolution system known as the Uniform Dispute Resolution Policy (UDRP). The UDRP has become the single most important mechanism for adjudicating disputes between those with an interest in a real world identifier, such as a registered trade mark, and domain name registrants.

8.1 Origins of the UDRP

The immediate roots of the UDRP lie in the June 1998 policy statement of the United States Department of Commerce, that led to the formation of ICANN. The statement did not recommend specific remedies for the complaints of trade mark owners, but instead proposed a process of international consultations on domain name dispute resolution to be conducted under the auspices of the World Intellectual Property Organization (WIPO).⁴⁸

⁴⁷ (2000) 202 CLR 45 at 66 referring to United States, *Restatement Third, Unfair Competition*, s 25, Comment (a).

⁴⁸ NTIA (1998) *op cit* note 136 at 31,747.

Pursuant to the recommendations, WIPO initiated a multi-staged consultative process to consider the future shape of a dispute resolution system. This process was quite different from the traditional functions performed by WIPO, which was confined to activities such as developing model national laws or preparing expert reports to support the development of international treaties. In effect, WIPO was acting in response to a request from an organ of a single government, the United States Department of Commerce, to convene a study to be submitted to a private corporation, ICANN, which could implement any proposals without further consultation with other national governments.

As a result of its consultative process, WIPO produced an *Interim Report* in December 1998⁴⁹ and a *Final Report* in April 1999.⁵⁰ The main recommendations of the WIPO *Final Report* were as follows:

- The adoption of a uniform dispute resolution policy, known as an ‘administrative procedure’, to be made mandatory through contractual clauses imposed on all domain name registrants in open gTLDs;
- The scope of the process to be limited to cases of deliberate, bad faith, abusive registration of trade marks as domain names, thereby effectively excluding proceedings alleging violations of trade names, geographical indications or personality rights;
- Complainants to be limited to trade mark holders;
- Remedies to be limited to cancellation or transfer of a domain name, and the allocation of costs, meaning that damages would not be available;
- Parties to retain the ability to initiate litigation in national courts, in which case the decision of the national court prevails over the administrative determination under the UDRP;
- UDRP determinations to be effectively self-executing, by the relevant registrars making the appropriate changes to the domain name system (DNS) database;
- Famous and well known marks to be excluded from registration as domain names.

The WIPO recommendations were submitted to the then newly-established ICANN, which began an expedited process to review the proposals. The review was undertaken by a working group of ICANN’s Domain Name Supporting Organization (DNSO). The board of ICANN accepted the working group’s recommendations and approved the final version of the UDRP, and the associated *Rules for UDRP*, in October 1999. ICANN essentially accepted the recommendations of the final WIPO report, with the notable exception of the recommendation for excluding famous and well known marks. Nevertheless, ICANN modified some of WIPO’s proposals, mainly by improving the position of domain name registrants as against trade mark owners in a number of ways, including:

⁴⁹ WIPO, *The Management of Internet Names and Addresses: Intellectual Property Issues*, Interim Report of the WIPO Internet Domain Name Process, December 23 1998.

⁵⁰ WIPO, *Final Report of the WIPO Internet Domain Name Process*, 30 April 1999, available at <http://wipo2.wipo.int/process1/report/index.html>.

- defining the circumstances in which a domain name registrant would not be acting in bad faith;
- requiring complainants to submit to the jurisdiction of national courts in either the nation in which the registrar had its principal office or nation of the domain name registrant's address; and
- including a definition of 'reverse domain name hijacking'.

8.2 Implementation of the UDRP

The ICANN UDRP establishes the substantive rules governing disputes between trade mark owners and domain name registrants. It is known as a 'mandatory administrative procedure'.⁵¹ The ICANN *Rules for UDRP*, approved at the same time as the UDRP, deal with procedural matters, including notice, appointment of a panel and timing of decisions. In late 1999, ICANN accredited three dispute settlement providers: WIPO, the National Arbitration Forum and eResolution. The CPR Institute for Dispute Resolution (CPR) was accredited in May 2000. eResolution went into voluntary bankruptcy in late 2001, and ceased accepting complaints from 30 November 2001. ICANN accredited a new dispute settlement provider, Asian Domain Name Dispute Resolution Centre, in February 2002. Each dispute settlement provider has supplemental rules, which deal with procedural matters, including communication with the dispute settlement provider. UDRP panelists supplied by the dispute settlement providers include practising lawyers, academics and retired members of the judiciary.

The UDRP was initially applied to disputes in the three original open gTLDs, .com, .net and .org. Disputes in all of the new gTLDs are to be subject to the UDRP. Some of the new gTLDs, including .biz, .info, and .name developed specific dispute resolution policies designed to resolve disputes during the 'start-up' phase of operation. The 'start-up' (or 'sunrise') policies were principally aimed at providing trade mark owners with additional protection during the initial stages of operation of the new domains. Adoption of the UDRP is imposed as a requirement under the ICANN accreditation agreement with registrars of gTLDs.⁵² All domain name registrants in the relevant gTLDs are contractually bound to submit to the UDRP. In addition to the gTLDs, the UDRP has been adopted by the managers of some ccTLDs, such as .nu, .tv and .ws. Other ccTLD administrations have adopted modified versions of the UDRP.

The first UDRP complaint was filed in December 1999 and the first decision issued in January 2000.⁵³ The first UDRP complaint in relation to the new gTLDs was filed in

⁵¹ UDRP, Paragraph 4.

⁵² See *November 1999 Registrar Accreditation Agreement* (applies to registrars accredited only in .com, .net and .org) clause II.K, available at <http://www.icann.org/registrars/ra-agreement-10nov99.htm>; *May 2001 Registrar Accreditation Agreement* (applies to registrars in .biz, .info and .name and to electing registrars in .com, .net and .org) clauses 3.8, 4, available at <http://www.icann.org/registrars/ra-agreement-17may01.htm>.

⁵³ *World Wrestling Federation Entertainment, Inc v Michael Bosman*, WIPO Case No D99-0001 (January 14, 2000).

October 2001 and the first decision issued in December 2001. By early April 2002, almost 5,500 complaints had been lodged under the UDRP in relation to over 9,000 domain names, and UDRP panelists had delivered over 4,500 decisions.⁵⁴ In 2001, there was a decline in the number of UDRP complaints lodged in relation to the original gTLDs, but this was more than off-set by complaints filed in relation to the new gTLDs.⁵⁵

8.3 Abusive Registration

If a complainant files a complaint with an accredited dispute resolution provider, the domain name registrant is contractually bound to submit to the ICANN UDRP. Paragraph 4a of the UDRP sets out the elements that a complainant must establish in order to make out a breach of the UDRP. To establish an abusive registration a complainant must prove the following three elements:

- the domain name is identical or confusingly similar to a trade mark or service mark in which the complainant has rights;
- the domain name registrant has no rights or legitimate interests in respect of the domain name; and
- the domain name has been registered and is being used in bad faith.

Although there is no formal system of precedent, the UDRP panel decisions interpreting the elements of abusive registration have resulted in the emergence of a distinctive form of international domain name jurisprudence. In effect, the UDRP establishes a new form of protection for trade marks (and related rights) insofar as they are used as domain names. In this sense, abusive registration under the UDRP may be seen as a form of ‘para-’ trade mark law – a system of rules that is separate from traditional intellectual property rights, but which protects those rights in the context of the Internet.

The general form in which the elements of abusive registration are expressed confers considerable discretion on UDRP panelists. An understanding of the elements of abusive registration therefore depends upon a consideration of the way in which panelists have come to interpret the elements and of the areas in which there have been inconsistent decisions. This section of the paper examines each of the elements in turn.

8.3.1 The First Element

There are two requirements that must be met in order for the first element of abusive registration to be satisfied: the domain name must be identical or confusingly similar to the trade mark; and the complainant must have rights in the trade mark.

⁵⁴ See ICANN, *Statistical Summary of Proceedings under Uniform Dispute-Resolution Policy*, available at <http://icann.org/udrp/proceedings-stat.htm> (accessed 4 April 2002).

⁵⁵ See WIPO, *WIPO Continues Efforts to Curb Cybersquatting*, Press Release PR/2002/303, February 26, 2002.

- **Domain name identical or confusingly similar to a trade mark**

In determining whether a domain name is identical to a trade mark, panelists have compared the alphanumeric domain name with the alphanumeric elements of the trade mark. For example, in *Chernow Communications, Inc v Jonathan D Kimball*,⁵⁶ the complainant was the owner of the registered trade mark ‘C-Com’ and the respondent was the registrant of the domain name <ccom.com>. The respondent argued that the domain name was not identical to the trade mark as it contained a hyphen. The majority of the panel determined that punctuation marks are to be disregarded in considering whether a domain name is identical. Similarly, design elements that may form part of a trade mark are to be ignored in deciding if the domain name is identical. Thus, in *General Machine Products Company, Inc v Prime Domains*,⁵⁷ the complainant was the owner of two registered trade marks for stylised versions of the word ‘CRAFTWORK’, while the respondent had registered the domain name <craftwork.com>. The panel held that the design elements of the mark were irrelevant for the purposes of determining whether the domain name was identical.

The practice of ‘typosquatting’, meaning inserting letters or symbols in a domain name so as to mislead Internet users who are attempting to access the correctly spelt URL, will generally be ignored when comparing the domain name with the trade mark. In almost all cases, typosquatting has been held to result in a domain name that is confusingly similar to the trade mark. For example, in *Oxygen Media, LLC v Primary Source*,⁵⁸ the respondent had registered the domain name <Oxygen.com>, substituting a zero for the ‘O’ in Oxygen. The panelist held that the domain name was calculated to trade on the complainant’s trade mark, Oxygen Media, and was confusingly similar to the mark. Similarly, in *Microsoft Corporation v Charlie Brown*,⁵⁹ the panelist held that the disputed domain name <microosoft.com> was confusingly similar to the ‘MICROSOFT’ trade mark. Moreover, in *Pfizer, Inc v Seocho and Vladimir Snezko*,⁶⁰ the panelist held that the addition of ‘www’ to the domain name was irrelevant for the purpose of comparing the name with the ‘PFIZER’ trade mark. The domain name was found to be confusingly similar to the mark.

National systems of trade mark law have developed principles for determining whether a mark is confusingly similar to a registered trade mark. The principles are designed to determine whether there is a likelihood of confusion as to the source of products associated with the mark. For instance, under Australian trade mark law, a mark will be ‘deceptively similar’ essentially if there is a real risk that use of the mark will result in a significant number of persons being confused as to the origin of goods. Thus, in *Shell Co of Australia Ltd v Esso Standard Oil (Australia) Ltd*, Windeyer J stated that:

⁵⁶ WIPO Case No D2000-0119 (May 18, 2000).

⁵⁷ NAF FA92531 (January 26, 2000).

⁵⁸ WIPO Case No D2000-0362 (June 19, 2000).

⁵⁹ WIPO Case No D2001-0362 (August 16, 2001).

⁶⁰ WIPO Case No D2001-1199 (November 28, 2001).

... the comparison is ... between, on the one hand, the impression based on recollection of the plaintiff's mark that persons of ordinary intelligence and memory would have; and on the other hand, the impressions that such persons would get from the defendant's ... exhibitions ... The likelihood of deception must be judged not by the degree of similarity alone, but by the effect of that similarity in all the circumstances.⁶¹

Under United States trade mark law, the courts take into account eight factors, known as the *Sleekcraft* factors, in deciding whether there is a likelihood of confusion with a registered trade mark.⁶²

The majority of panel decisions have not applied principles developed in the context of trade mark law in deciding whether a domain name is 'confusingly similar' for the purposes of the UDRP. This is because the issue under the UDRP is not whether there is confusion as to the origin of goods, but simply whether the domain name is 'confusingly similar' to the trade mark. In determining whether a domain name is 'confusingly similar', the panelists therefore focus on similarities between the alphanumeric domain name and the trade mark. For example, in *Wal-Mart Stores, Inc v Richard MacLeod d/b/a For Sale*,⁶³ the domain name under dispute was <wal-martsucks.com>. The panelist followed previous determinations in concluding that the addition of another word in a domain name, such as 'sucks', meant that the name was not identical to the trade mark. The complainant argued that any domain name incorporating 'wal-mart' would cause consumers to believe that there was an association with the trade mark owner. The panelist, however, held that, as the UDRP was directed at preventing cybersquatting, and not directly at preventing trade mark infringement, a likelihood of confusion as to the source of the name was not the issue. Rather, what is required is a direct comparison between the domain name and the trade mark. In concluding that, in this case, the domain name was confusingly similar to the trade mark, the panelist stated that:

... a domain name is "identical or confusingly similar" to a trademark for the purposes of the Policy when the domain name includes the trademark, or a confusingly similar approximation, regardless of the other terms in the domain name. In other words, the issue under the first factor is not whether the domain name causes confusion as to source (a factor more appropriately considered in connection with the legitimacy of interest and bad faith factors), but instead whether the mark and domain name, when directly compared, have confusing similarity.⁶⁴

A similar approach was adopted in *Nicole Kidman v John Zuccarini, d/b/a Cupcake Party*,⁶⁵ in which the domain name <nicolekidmannude.com> was held to be confusingly similar to the name 'Nicole Kidman'. The majority of the panel maintained that the issue

⁶¹ (1963) 109 CLR 407 at 415-416.

⁶² See *AMF Inc v Sleekcraft Boats*, 599 F 2d 341 (1979).

⁶³ WIPO Case No D2000-0662 (January 23, 2001).

⁶⁴ *Ibid.* para 6.

⁶⁵ WIPO Case No D2000-1415 (January 23, 2001).

was not whether the names were confusing for the purposes of national trade mark law, but whether the names were confusing in the context of cybersquatting. Accordingly, the majority observed that:

... the Policy is not focused on the narrow question of “whether the domain name causes confusion as to source” ... but rather on the broader question of whether a domain name is similar enough in light of the purpose of the Policy to justify moving on to the other elements of a claim for cancellation or transfer of a domain name.⁶⁶

A minority of panels have applied principles derived from national trade mark laws in determining whether a domain name is confusingly similar. Panelists that have adopted this approach seem, without exception, to have applied the United States *Sleekcraft* factors. Panel decisions that have followed United States law appear to have been influenced by the extent to which the *Sleekcraft* factors have been used to compare domain names and trade marks under United States trade mark law and under the United States *Anticybersquatting Consumer Protection Act*. For example, in *Wal-Mart Stores, Inc v Walsucks and Walmarket Puerto Rico*,⁶⁷ the panelist applied United States trade mark law to find that a number of domain names, including <walmartcanadasucks.com> were confusingly similar to the ‘WAL-MART’ trade mark. In adopting this approach, the panelist failed to consider the appropriateness of applying a test developed for determining the likelihood of confusion between two marks in the context of a policy aimed at preventing cybersquatting.⁶⁸ It is noteworthy that a subsequent decision, *Wal-Mart Stores, Inc v walmartcanadasucks.com and Kenneth J Harvey*,⁶⁹ that also applied United States trade mark law, concluded that the domain name <walmartcanadasucks.com> was not confusingly similar to the ‘WALMART’ trade mark. The panelist in that case applied the *Sleekcraft* factors, but emphasised different factors to those considered significant by the panelist in the <walmartcanadasucks.com> decision.

▪ Trade mark or service mark in which the complainant has rights

The scope of the UDRP is confined to disputes between trade mark owners and domain name registrants. Disputes concerning areas where there is much less harmony between national laws than is the case with trade mark law, such as protection of personal names, geographical indications and trade names, were deliberately set aside by WIPO in the report which led to ICANN adopting the UDRP. Thus, the WIPO report stated that:

... registrations that violate trade names, geographical indications or personality rights would not be considered to fall within the definition of abusive registration

⁶⁶ *Ibid.* para 5.

⁶⁷ WIPO Case No D2000-0477 (July 20, 2000).

⁶⁸ The panelist simply stated that: ‘The question whether a domain name and a trademark are confusingly similar involves the application of a multifactor test exemplified in the decision of the US Court of Appeals for the Ninth Circuit in *AMF Inc v Sleekcraft Boats*, 599 F 2d 341 (1979)’: *ibid.* para 6.

⁶⁹ WIPO Case No D2000-1104 (November 23, 2000).

for the purposes of the administrative procedure. Those in favor of this form of limitation pointed out that the violation of trademarks (and service marks) was the most common form of abuse and that the law with respect to trade names, geographical indications and personality rights is less evenly harmonized throughout the world, although international norms do exist requiring the protection of trade names and geographical indications. We are persuaded by the wisdom of proceeding firmly but cautiously and of tackling, at the first stage, problems which all agree require a solution ... we consider that it is premature to extend the notion of abusive registration beyond the violation of trademarks and service marks at this stage.⁷⁰

Issues relating to the protection of trade names, geographical indications and personal names were taken up in the Second WIPO Domain Name Process, which resulted in a final report released in September 2001. Nevertheless, some of these issues have emerged in the interpretation of the UDRP, albeit in another guise. Although it was always clear that the UDRP extended to unregistered trade marks, as well as to registered marks, questions have arisen concerning the extent to which the UDRP applies to unregistered indicia. In particular, questions have arisen in relation to the protection of famous or well-known personal names and the protection of geographical names.

Famous or well-known personal names

A number of decisions have concerned the extent to which the UDRP extends to famous or well-known personal names. The issue in these decisions has been whether the personal name can be protected as an unregistered mark. The most significant decision extending protection to a famous name is *Jeanette Winterson v Mark Hogarth*,⁷¹ which concerned domain names that featured the well-known author's name, including <jeanettewinterson.com>. The panelist pointed out that the requirement that the complainant have rights in a trade mark did not mean that the mark must be registered. He held that the term 'trade mark', as used in the UDRP, is to be construed broadly to include, for example, the common law right to prevent unauthorised use of a name. The panelist referred to cases under English law in which the action for passing off had been applied to protect the names of well-known individuals and personalities, to conclude that the complainant would have an action to prevent unauthorised use of her name under English law. As the complainant would be able to protect the use of the name under English law, the panelist held that she had sufficient rights in the mark, consisting of her name, to satisfy the requirements of the UDRP. A majority of UDRP decisions have followed the *Jeanette Winterson* decision in regarding the UDRP as protecting famous personal names. For example, in *Julia Fiona Roberts v Russell Boyd*,⁷² the panel cited the *Jeanette Winterson* decision for the proposition that common law trade mark rights

⁷⁰ WIPO (1999) *op cit* paras 167-8, p 45.

⁷¹ WIPO Case No D2000-0235 (May 22, 2000).

⁷² WIPO Case No D2000-0210 (May 29, 2000).

exist in an author's name and, with very little discussion of the issue, concluded that Julia Roberts had rights in her personal name sufficient to confer standing under the UDRP.⁷³

A minority of panel decisions have expressed reservations about whether the UDRP should be interpreted as protecting famous personal names. For example, in *Bruce Springsteen v Jeff Burgar and Bruce Springsteen Club*,⁷⁴ which concerned the domain name <bruce.springsteen.com>, the majority of the panel stated that 'it is by no means clear from the UDRP that it was intended to protect proper names of this nature'.⁷⁵ As the majority held against the musician, Bruce Springsteen, on another ground, they did not pursue the matter.⁷⁶ Moreover, in *Gordon Sumner, p/k/a Sting v Michael Urvan*,⁷⁷ the panelist suggested that a celebrity may not have rights to a name if the name has a number of other meanings. In that decision, the issue was the rights of the well-known pop star, 'Sting', to the domain name <sting.com>. The panelist cited the 1999 WIPO report as authority for the proposition that the UDRP was not intended to apply to personality rights. He distinguished the line of decisions extending protection to famous personal names on the basis that the word 'sting' is a common word in the English language with a number of meanings. Nevertheless, the panelist concluded that it was unnecessary to make a definitive finding on the issue as the complainant failed to establish that there was an abusive registration on another ground.

Geographical names

A number of panel decisions have dealt with the extent to which geographical names fall within the scope of the UDRP. There have been two main issues in decisions involving domain names that include a geographical name: whether a geographical name can be protected as an unregistered trade mark; and whether a domain name that includes a geographical name is confusingly similar to a registered trade mark that contains the geographical name.

Most panel decisions have concluded that a geographical name will usually not amount to an unregistered trade mark. For example, in *Brisbane City Council v Warren Bolton Consulting Pty Ltd*,⁷⁸ the Brisbane City Council filed a complaint in relation to the domain name <brisbanecity.com>. The complainant alleged that 'BRISBANE CITY' was an unregistered trade mark to which the UDRP applied. It also contended that the domain name was confusingly similar to its registered trade mark, 'BRISBANE CITY WORKS'. The panelist held that, in determining whether a geographical name is an unregistered trade mark, the crucial issue is whether the name is performing the function

⁷³ To like effect see *Rudner v Internetco Corp.* WIPO Case No D2000-0581 (August 3, 2000) (<ritarudner.com>); *CMG Worldwide, Inc v James Dean Internet Club* NAF FA94187 (April 11, 2000) (<jamesdean.net>); *Carter v Afternoon Fiasco* WIPO Case No D2000-0658 (October 17, 2000) (<nikcarter.com>); *Feinstein v PAWS Video Productions* WIPO Case No D2000-0880 (October 21, 2000) (<michael feinstein.com>).

⁷⁴ WIPO Case No D2000-1532 (January 25, 2001).

⁷⁵ *Ibid.* para 6.

⁷⁶ The minority in the *Bruce Springsteen* decision disagreed with the majority's reservations.

⁷⁷ WIPO Case No D2000-0596 (July 20, 2000).

⁷⁸ WIPO Case No D2001-0047 (May 7, 2001).

of a trade mark, meaning that the mark is being used to distinguish the goods and services of the complainant from those of other traders. In this case, the name ‘BRISBANE CITY’ was found to describe a geographical location but, as there were many traders operating in the City of Brisbane, it did not perform the function of a trade mark.⁷⁹ The panelist further decided that the domain name was not confusingly similar to the registered trade mark, ‘BRISBANE CITY WORKS’, essentially because the words ‘BRISBANE CITY’ were not, in themselves, distinctive.

The *Brisbane City* reasoning was recently applied in *Stadt Heidelberg v Media Factory*,⁸⁰ which concerned a complaint from the City of Heidelberg in relation to the domain name <heidelberg.net>. The panelist summarised the effect of the line of decisions dealing with geographical names in the following terms:

Each of those cases rested upon a showing that by virtue of the activities carried on by the Complainant, the geographical name either with, or without additional matter, had come to denote the goods or service of Complainant, and had acquired the character of a trade mark.⁸¹

The panelist concluded that, as there was no evidence that the name ‘HEIDELBERG’ had become distinctive as a trade mark, it could not be considered an unregistered mark for the purposes of the UDRP. An interesting feature of the decision is that the Regional Court of Mannheim had previously held that the City of Heidelberg was entitled to the domain name <heidelberg.de> and the ccTLD for Germany.

The position is, nevertheless, different where a complainant has registered trade marks that include a geographical name. The best known decision concerning a registered geographical name is *Excelentísimo Ayuntamiento de Barcelona v Barcelona.com Inc*,⁸² in which the city government of Barcelona lodged a complaint in relation to the domain name <barcelona.com>. In that decision, the complainant had numerous registered trade marks under Spanish trade mark law that included the component ‘BARCELONA’. The panelist held that, as the principal element or distinctive character of the registered marks was the word ‘BARCELONA’, the domain name was confusingly similar.⁸³

8.3.2 The Second Element

The second element that needs to be established under the UDRP is that the domain name registrant has no rights or legitimate interests in the domain name. As this involves establishing a negative, it naturally raises procedural issues, including issues relating to

⁷⁹ See also *Brisbane City Council v Joyce Russ Advertising Pty Ltd* WIPO Case No D2001-0069 (May 14, 2001); *Chambre de Commerce et d’Industrie de Rouen v Marcel Stenzel* WIPO Case No D2001-0348.

⁸⁰ WIPO Case No D2001-1500 (March 6, 2002).

⁸¹ *Ibid.* para 7.2.

⁸² WIPO Case No D2000-0505 (August 4, 2000).

⁸³ See also *Kur- und Verkehrsverein St Moritz v StMoritz.com* WIPO Case No D2000-0617 (August 17, 2000) (<stmoritz.com>).

the burden of proof. Two further related questions arise in interpreting the second element of abusive registration:

- What amounts to ‘rights or legitimate interests’? and
- Which law should be applied to determine whether a domain name registrant has rights or legitimate interests in the name?

▪ **Burden of Proof**

The second element of abusive registration is important because it establishes the basic principle that the UDRP is concerned only with disputes where the registrant has no interest whatsoever in the domain name, and not with determining a competition on the merits between competing claims to a domain name. In effect, this element is a sort of defence – if the registrant has a recognisable right or interest in the domain name, the complainant’s case falls down. Nevertheless, under paragraph 4a of the UDRP, the complainant bears the onus of proving each of the three elements of abusive registration.

Panel decisions dealing with the second element of abusive registration have recognised the difficulties facing a complainant required to establish the negative proposition that the registrant has no rights or interests. Consequently, the complainant need only make out a prima facie case that the registrant has no legitimate interest, whereupon the burden of proof shifts to the respondent, who must produce evidence of an interest in the name.⁸⁴ The complainant may satisfy the initial burden merely by asserting that the respondent has no interest and producing some evidence of cybersquatting.⁸⁵ If a respondent fails to respond to a complaint and a prima facie case of no legitimate interest has been established, the panel will find against the respondent.⁸⁶ In part, this is because, in the event of default, the panel can accept the facts as pleaded⁸⁷ and because the panel can draw an adverse interest from a failure to respond.⁸⁸ If the complainant fails to make out a prima facie case of no interest, however, the panel will find for the respondent.⁸⁹

▪ **No rights or legitimate interests**

The UDRP does not attempt to define what is meant by a right or legitimate interest in a domain name. Nevertheless, paragraph 4c of the UDRP lists the following three non-exclusive examples of what may amount to a right or legitimate interest:

- use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services;

⁸⁴ *Document Technologies, Inc v International Elec. Communications Inc* WIPO Case No D2000-0270 (June 6, 2000).

⁸⁵ *Inter-Continental Hotels Corp. v Soussi* WIPO Case No D2000-0252 (July 5, 2000).

⁸⁶ See *Nicole Kidman v John Zuccarini, d/b/a Cupcake Party* WIPO Case No D2000-1415 (January 23, 2001).

⁸⁷ *Talk City, Inc v Robertson* WIPO Case No D2000-0009 (February 29, 2000).

⁸⁸ *Alcoholics Anonymous World Services, Inc v Raymond* WIPO Case No D2000-0007 (March 6, 2000).

⁸⁹ *EAuto, LLC v EAuto Parts* WIPO Case No D2000-0096 (April 9, 2000).

- the respondent being commonly known by the domain name, even if it has acquired no trade mark or service mark rights; or
- making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trade mark or service mark at issue.

UDRP decisions have expanded upon the meaning of some of the terms used in the examples given of rights or legitimate interests.

Demonstrable preparations

Evidence that the respondent has developed a business plan that includes the use of the domain name, and purchase of the domain name in pursuance of the business plan, will indicate that demonstrable preparations have been taken to use the name. For example, in *Physik Instrumente GmbH & Co v Kerner*,⁹⁰ the respondents, a new media and Internet consultancy, developed a proposal for an Internet portal to be labelled 'pi.com'. The proposal was evidenced by a document stored on a computer. The respondents later purchased the domain name <pi.com>. The panelist held that the complainant had failed to establish that the respondents had no legitimate interest in the domain name, even though the respondents subsequently decided not to pursue the business plan.⁹¹ On the other hand, mere assertions of preparations to use a domain name, without further evidence, will not be considered sufficient to establish that the respondent has undertaken demonstrable preparations to use the name. In particular, non-use of a domain name for a significant time after registration will be likely to result in a finding that there have been no demonstrable preparations to use the name. For example, in *Helen Fielding v Anthony Corbert aka Anthony Corbett*,⁹² the respondent claimed the he planned to develop the domain name <bridgetjones.com> into a fan site. As two years had elapsed since registration of the site, and no evidence had been produced of preparations to use the site, the panelist found that the respondent had no legitimate interest in the domain name.⁹³

Bona fide offering of goods and services

The clearest evidence of use of a domain name in connection with a bona fide offering of goods or services is if the Web-site identified by the domain name actually offers goods or services. Moreover, using the Web-site to advertise goods or services supplied off-line will amount to a bona fide offering. Thus, in *EAuto, LLC v EAuto Parts*,⁹⁴ the respondent used the Web-site <eautoparts.com> to advertise its business of maintaining and repairing automobiles. Even though the site was not active at the time of the decision, and even though the respondent failed to file a response, the panel concluded

⁹⁰ WIPO Case No D2000-1001 (October 3, 2000).

⁹¹ See also *Safmarine v Network Management* WIPO Case No D2000-0764 (October 23, 2000).

⁹² WIPO Case No D2000-1000 (September 25, 2000).

⁹³ See also *World wrestling Federation Entertainment, Inc v Ringside Collectibles* WIPO Case No D2000-1306 (January 24, 2001).

⁹⁴ WIPO Case No D2000-0096 (April 9, 2000).

that the complainant had failed to establish that there was no legitimate interest in the domain name.

Use of a domain name to resell goods or services will not amount to a bona fide offering where the respondent is not an authorised reseller. For example, in *Raymond Weil SA v Watchesplanet (M) Sdn Bhd*,⁹⁵ the respondent used the domain name <raymon-weil-watches.com> to sell watches manufactured by the complainant which had been acquired in the ‘grey’ market. The panelist held that, as use of the complainant’s trade mark was not authorised, there was no bona fide use of the domain name. Furthermore, in *Universal City Studios, Inc v GAB Enterprises*,⁹⁶ the panelist held that an offering of goods or services is not bona fide if use of the domain name is likely to cause consumer confusion to the extent that it would infringe the complainant’s trade mark rights. In that decision, the respondent was the registered owner of the domain name <fieldofdreams.com>, which it used to provide baseball news and to advertise sports memorabilia. The panelist concluded that, although the site was used to offer goods or services, the offering was not bona fide, as use of the site was likely to cause confusion with the complainant’s registered trade mark. A number of factors meant that confusion was likely, including a link to a Web site of the complainant, which was devoted to the movie, ‘Field of Dreams’.

Domain name speculation

Registration of a domain name for the purpose of speculating in domain names that consist of generic words may be sufficient to constitute a legitimate interest in the name. For example, in *Micron Technology, Inc v Null International Research Center*,⁹⁷ the respondent was in the business of registering and offering domain names for sale. The panelist held that domain name speculation could be a legitimate interest provided the respondent is unaware of the complainant’s trade mark rights. As the respondent had registered a number of domain names similar to the name at issue, and there was no evidence that it knew of the complainant’s trade mark, the panelist held that it had not been established that there was no legitimate interest in the domain name <crucialtechnology.com>.⁹⁸ In *Toronto Star Newspapers Limited v Virtual Dates Inc*,⁹⁹ the respondent was in the business of warehousing and using generic domain names. The respondent registered the domain name <tstv.com>, which appeared to be used primarily to re-direct users to cyberporn sites. The complainant, the registered owner of the trade mark ‘TSTV’, alleged that the respondent had no legitimate interest in the domain name. The panel, however, held that as ‘tstv’ was an accepted abbreviation of ‘transsexual and transvestite’, the domain name was being used in connection with a bona fide offering of services.

⁹⁵ WIPO Case No D2001-0601 (June 30, 2001).

⁹⁶ WIPO Case No D2000-0416 (June 30, 2000).

⁹⁷ WIPO Case No D2001-0608 (June 20, 2001).

⁹⁸ See also *General Machine Products Co v Prime Domains* NAF FA92531 (January 26, 2000); *Kis v Anything .com Ltd* WIPO Case No D2000-0770 (November 20, 2000); *Audiopoint, Inc v eCorp a/k/a Chad Folkening* WIPO Case No D2001-0509.

⁹⁹ WIPO Case No D2000-1612 (February 6, 2001).

Domain name speculation will not amount to a legitimate interest, however, if the domain name has been registered with an intent to profit from, or otherwise abuse, the complainant's trade mark rights. This principle was first established in *Allocation Network GmbH v Steve Gregory*.¹⁰⁰ In that decision, the respondent registered numerous generic names, including <allocation.com>, which it offered for sale. The panelist held that, as there was no evidence to suggest that the respondent knew, or should have known, of the complainant's German trade mark 'ALLOCATION', the domain name had not been registered with an intent to profit or abuse the complainant's trade mark rights. Accordingly, the complainant had not established that the respondent had no legitimate interest in the domain name. In *J. Crew International, Inc v crew.com*,¹⁰¹ the respondent engaged in the business of domain name speculation and, to that end, registered the domain name <crew.com>. The complainant was the owner of United States trade marks, including 'J. CREW' and 'CREW', which were registered in relation to clothing and accessories. The only use of the domain name by the respondent was the placement of a banner ad on the Web-site, which linked to the complainant's site. The majority of the panel decided that, as the respondent had constructive notice of the complainant's trade mark rights, it had no legitimate interest in the domain name. While acknowledging that domain name speculation may be a legitimate interest, the majority proposed a test for determining when speculation will not be legitimate:

... registration of domain names for speculative purposes constitutes an abusive registration when (1) the respondent has no demonstrable plan to use the domain name for a bona fide purpose prior to registration or acquisition of the domain name; (2) the respondent had constructive or actual notice of another's rights in a trademark corresponding to the domain name prior to registration or acquisition of the domain name; (3) the respondent engages in a pattern of conduct involving speculative registration of domain names; and (4) the domain name registration prevents the trademark holder from having a domain name that corresponds to its registered mark.¹⁰²

In that decision, a strong dissent by the minority maintained that the proposed test would reduce the issue in decisions dealing with domain name speculation to whether the respondent had a demonstrable plan to use the domain name for a bona fide purpose prior to registration. The test proposed by the majority has not been taken up in subsequent panel decisions.

Freedom of expression and criticism sites

A degree of inconsistency has emerged in panel decisions dealing with whether the registrant of a domain name for a site that includes criticism of a trade mark owner has a legitimate interest in the name. A number of decisions have held that criticism is a legitimate noncommercial or fair use of a domain name for the purposes of the UDRP.

¹⁰⁰ WIPO Case No D2000-0016 (March 24, 2000).

¹⁰¹ WIPO Case No D2000-0054 (April 20, 2000).

¹⁰² *Ibid.* para 7.

Some panels have also decided that the exercise of free speech for criticism and commentary is a separate basis for finding that a respondent has a legitimate interest in a domain name.

Among the ‘free speech’ decisions, one of the most important is *Bridgestone Firestone, Inc v Jack Myers*.¹⁰³ In that decision, the respondent registered the domain name <bridgestone-firestone.net>. The respondent was a former employee of the complainant, a rubber tyre manufacturer and owner of numerous registered trade marks that include the words ‘BRIDGESTONE’ and ‘FIRESTONE’. The respondent used the site for news articles, for a consumer/employee forum, and for a range of other material critical of the complainant. The panelist decided that use of the domain name for criticism was a fair use under the UDRP. The panelist also decided that the respondent’s use of the site for criticism was an exercise of free speech rights that amounted to a legitimate interest in the domain name. In this respect, the panelist stated that:

Although free speech is not listed as one of the Policy’s examples of a right or legitimate interest in a domain name, the list is not exclusive, and the Panel concludes that the exercise of free speech for criticism and commentary also demonstrates a right or legitimate interest in the domain name under Paragraph 4(c)(iii). The Internet is above all a framework for global communication, and the right to free speech should be one of the foundations of Internet law.¹⁰⁴

The decision made it clear that use of the ‘.net’ gTLD, rather than ‘.com’, was significant in finding that the use of the name amounted to a legitimate noncommercial and fair use.

Even if a domain name is not directly used for criticism, a respondent may have a legitimate interest in the name based on fair use and free speech considerations. In *Bloomberg LP v Secaucus Group*,¹⁰⁵ the domain name <michaelbloomborgsucks.com> re-directed users to the <sucks.com> Web-site, which was established to allow users to register complaints about corporate America, politicians and celebrities. The majority of the panel decided that use of the domain name was both a fair use and an exercise of free speech for criticism and commentary. The decision was clearly influenced by the inclusion of the ‘sucks’ suffix in the domain name, which seems almost always to amount to an exercise of free speech rights or fair use.

The *Bloomberg* decision may be usefully contrasted with the decision in *PG&E Corporation v Samuel Anderson*.¹⁰⁶ In that decision, the respondent registered a number of domain names, including <pge2000.com>. The <pge2000.com> Web-site included material criticising the complainant, Pacific Gas and Electric. Nevertheless, the Web-site also included a notice advertising for sale a number of domain names that included variations of the complainant’s ‘PG&E’ trade mark. The panelist rejected the respondent’s claim that it had a fair use or free speech interest in the domain name on the

¹⁰³ WIPO Case No D2000-0190 (July 6, 2000).

¹⁰⁴ *Ibid.* para 6.

¹⁰⁵ NAF FA97077 (June 7, 2001).

¹⁰⁶ WIPO Case No D2000-1264 (November 22, 2000).

basis that the domain name was used for the commercial purpose of offering domain names for sale. In concluding that there was no legitimate interest in the domain name, the panelist maintained that the respondent was ‘not free to use Complainant’s mark to attract Internet users to its website where it offers domain names confusingly similar to Complainant’s registered marks for sale’.¹⁰⁷ A similar conclusion was reached in *Rolex Watch USA, Inc v Spider Webs, Ltd*,¹⁰⁸ which concerned the domain names <relojesrolex.com> and <erolexwatches.com>. The domain names resolved to the Web-site <spintopic.com>, which allegedly provided a forum for consumer information. The panel found that there was no fair use of the domain names primarily because there was no commentary on Rolex watches on the ‘spintopic’ Web-site.

A number of decisions have concluded that even where a site is used for legitimate criticism, the respondent has no legitimate interest in the domain name. In most of these decisions, there has been some indication of a commercial use of the site over and above use of the site for criticism and commentary. For example, in *Monty and Pat Roberts, Inc v J Bartell*,¹⁰⁹ the respondent registered the domain name <montyroberts.org>. The complainant, Monty Roberts, was a well-known horse trainer, who provided horse training services and associated merchandise. The site was used for a number of purposes, including publishing information critical of Monty Roberts, linking to a Web-site that advertised ‘anti-Monty Roberts’ merchandise and linking to Web-sites advertising the services of other horse trainers. The panelist decided that, although there was a right to establish criticism sites, in this instance the respondent had used the domain name to identify itself with the complainant and attract users to its Web-site. The crucial factor in the decision seemed to be that the respondent was using the site to attract users so as to directly or indirectly offer products for sale. Similar reasoning was used in *The New York Times Company v New York Internet Services*¹¹⁰ to deny that the respondent had a legitimate interest in the domain name <newyorktimes.com>. In that decision, the intended use of the site was apparently to solicit comment and opinions on the New York Times. The site included banner advertisements linking to a site run by a Web hosting company, which the respondent provided as part of an agreement for free Web hosting. The panelist concluded that, as the respondent received financial benefits from the banner advertisements, its use of the domain name was not a noncommercial or fair use.

In some decisions panels have either decided that free speech considerations are outside of the scope of the UDRP, or have ignored the issue altogether. In *Mission KwaSizabantu v Benjamin Rost*¹¹¹ the respondent used domain names including <kwasizabantu.com> to publish critical views of the complainant, Mission KwaSizabantu. The panelist maintained that the ‘boundaries of free speech’ were outside the scope of UDRP adjudications. He concluded that there was no fair use of the domain name as use of the site for criticism amounted to tarnishing the activities associated with

¹⁰⁷ *Ibid.* para 6.

¹⁰⁸ WIPO Case No D2001-0398 (July 2, 2001).

¹⁰⁹ WIPO Case No D2000-0300 (June 29, 2000).

¹¹⁰ WIPO Case No D2000-1072 (December 5, 2000).

¹¹¹ WIPO Case No D2000-0279 (June 7, 2000).

the complainant's trade mark. In *Reg Vardy Plc v David Wilkinson*¹¹² the complainant was a large car sales business and owner of the trade mark 'REG VARDY', which was registered under United Kingdom trade mark law. The respondent, a disgruntled customer, registered the domain names <reg-varidy.com>, <reg-varidy.net> and <reg-varidy.org>. The domain names all resolved to the one site, which contained material critical of the car sales company. The panelist concluded that the respondent was using the domain names to divert business from the complainant's site. Without giving any consideration to free speech issues, the panelist concluded that the names had been registered solely to harm the complainant and that the respondent had no rights or legitimate interests in the domain names. The *Reg Vardy* decision may be usefully contrasted with the decision in *TMP Worldwide Inc v Jennifer L Potter*.¹¹³ In that decision, the respondent, a dissatisfied customer of TMP Worldwide, a Yellow Pages advertising agency, registered the domain names <tmpworldwide.net> and <tmpworldwide.org>. The respondent posted a letter on the Web sites complaining that the complainant had mishandled her Yellow Pages advertising account. The panelist concluded that the UDRP did not apply to use of a domain name involving commentary, comparative advertising, criticism, parody or news reporting. In other words, any of these activities would amount to a legitimate noncommercial use of the domain name at issue.¹¹⁴

▪ Choice of law

The *UDRP Rules* provide that decisions are to be made on the basis of the documents submitted by the parties, and any rules and principles of law that the panel deems applicable.¹¹⁵ This provides UDRP panels with considerable discretion in deciding which national legal principles to apply, or if any national legal principles should be applied at all, in resolving disputes between trade mark owners and domain name registrants. Nevertheless, the choice of legal authority may well be determinative of crucial issues raised in a UDRP dispute. This is, perhaps, most clearly seen in disputes involving criticism sites. Panelists applying United States legal principles tend to give great weight to free speech considerations in such decisions, as a result of the importance of First Amendment principles under United States law. Panelists from jurisdictions other than the United States, on the other hand, generally appear to place less importance on free speech considerations.

UDRP panels have varied considerably in the degree of sensitivity shown in applying national legal principles. In general terms, United States panelists appear to have been less constrained in applying principles derived from domestic United States law than panelists from other jurisdictions have been in applying principles derived from their own legal systems. The use of national legal principles in UDRP decisions would seem to raise two related issues. First, if inconsistent national principles are applied on a regular

¹¹² WIPO Case No D2001-0593 (July 3, 2001).

¹¹³ WIPO Case No D2000-0536 (August 5, 2000).

¹¹⁴ See also *Britannia Building Society v Britannia Fraud Prevention* WIPO Case No D2001-0505 (July 6, 2001).

¹¹⁵ *UDRP Rules*, clause 15(a).

basis, there is the potential for the predictability and consistency of UDRP decisions to be undermined. Second, an unthinking application of principles derived from national trade mark laws may not be appropriate in the context of a system of dispute resolution aimed at preventing cybersquatting. In fact, many UDRP decisions appear to display an underlying ambiguity in relation to the extent to which the UDRP is seen as a means for preventing trade mark infringement or for preventing cybersquatting. To an extent, the views adopted as to the fundamental purpose of the UDRP will invariably influence the interpretation placed on the elements of abusive registration. In short, the mechanical and wholesale application of principles derived from United States trade mark law is unlikely to advance the development of an international jurisprudence relating to cybersquatting.

8.3.3 The Third Element

The third, and probably most significant, element of abusive registration is the requirement of bad faith registration and use of the domain name. Two main issues have arisen in UDRP decisions in relation to the interpretation of the third element:

- Whether the domain name must be registered *and* used in bad faith; and
 - What amounts to ‘bad faith’ in the context of abusive domain name registration.
-
- **Registration and use**

Sub-paragraph 4(a)(iii) of the UDRP expressly requires a complainant to establish that the domain name has been registered *and* is being used in bad faith. This suggests that so-called ‘passive warehousing’, meaning merely registering the domain name without using it, is not enough to satisfy the third element of abusive registration.

In adopting the wording of the third element, ICANN deliberately refrained from changing the form of words proposed in the WIPO *Final Report* of April 1999. In particular, ICANN refused to accept the proposal of the International Trademark Association (INTA) to change the ‘*and*’ in the third element to ‘*or*’. INTA were concerned that the policy would not encompass bad faith warehousing, or bad faith use of a domain name following an initial good faith registration. Against this, others argued that mere registration of a domain name should not amount to trade mark infringement, as it is use of a mark that is of most concern to trade mark owners. It was also contended that it is impossible to determine whether registration of a domain name is in bad faith without also taking into account the use to which the name is put. The issue was so controversial that the ICANN drafting committee was completely deadlocked. In the end, ICANN counsel, Louis Touton, single-handedly decided the issue in favour of retaining use of ‘*and*’ rather than ‘*or*’.

In practice, the ICANN debates in relation to this issue have meant very little, as almost all panels have interpreted the ‘*and*’ in the third element to mean ‘*or*’. The decision which established this interpretation of the scope of abusive registration is *Telstra*

Corporation v Nuclear Marshmallows,¹¹⁶ one of the first decisions to be made under the UDRP, the most-cited decision and probably the most influential panel decision. In that case, the respondent registered the domain name <telstra.org>, which at no time resolved to an active Web-site. The decision of the panelist is complex and bears close reading. First, the panelist acknowledged that the clear wording of the UDRP requires both bad faith registration *and* bad faith use of the domain name. He pointed out that this was confirmed by the use of both past and present tenses in the third element of abusive registration. In other words, the third element requires that the domain name *has been* registered in bad faith and *is being* used in bad faith. Second, the panelist separated considerations relating to registration from considerations relating to use. In relation to registration, he essentially concluded that, given the well-known reputation of Telstra, it was not possible to conceive of circumstances in which the domain name could be legitimately used and, furthermore, that it was not possible to conceive of the respondent being unaware of this at the time of registration. In relation to use, the panelist concluded that the issue was not whether the domain name was being actively used in bad faith, but whether the respondent was, in all the circumstances, acting in bad faith. By applying this interpretation to the policy, the panelist was able to conclude that inactivity in relation to a domain name registered in bad faith could amount to bad faith use. The panelist concluded that the respondent was acting in bad faith because the trade mark has a strong reputation, there was no evidence of actual or contemplated good faith use, the registrant took active steps to conceal his true identity and failed to correct false details, and it was not possible to conceive of any use that would not be illegitimate. Although the reasoning in the decision was carefully nuanced, however, it cannot disguise the fact that it effectively extended the scope of the UDRP to apply to bad faith registration *per se*. Moreover, subsequent UDRP decisions have often tended to assume that bad faith registration accompanied by passive warehousing invariably satisfies the requirements of the third element of abusive registration.¹¹⁷

A number of decisions have held that the third element will not be made out where there has been a bad faith use of a domain name, but registration of the name was not in bad faith. For example, in *e-Duction, Inc v John Zuccarini*,¹¹⁸ the respondent registered the domain name <eduction.com>, which was used to re-direct users to sites containing advertisements, including advertisements for credit cards and music downloads. The complainant, a credit card company, later filed applications to register the trade mark 'E-DUCTION'. The panel concluded that, as the respondent was unaware of the complainant's mark at the time of registration, registration had not been in bad faith. Thus, even though use of the domain name to advertise credit cards was evidence of bad faith use, the third element of abusive registration had not been made out.

¹¹⁶ WIPO Case No D2000-0003 (February 18, 2000).

¹¹⁷ See, for example, *JP Morgan & Co v Resource Marketing* WIPO Case No D2000-0035 (March 23, 2000).

¹¹⁸ WIPO Case No D2000-1369 (February 5, 2001).

- **Bad faith**

Paragraph 4b of the UDRP lists four non-exclusive circumstances that are evidence of registration and use of a domain name in bad faith. While the first three circumstances appear to apply only to registration, the fourth listed circumstance applies only to use of a domain name. The four circumstances are:

- Registration or acquiring the domain name for the purpose of selling, renting or transferring the name to the complainant trade mark owner, or to a competitor of the complainant, for more than the respondent's out-of-pocket expenses directly related to the domain name;
- A pattern of conduct of registering domain names to block registration by a trade mark owner;
- Registration of the domain name primarily for the purpose of disrupting the business of a competitor; or
- Using the domain name to intentionally attract Internet users for commercial gain by creating a likelihood of confusion with the complainant's trade mark.

The four listed circumstances are illustrative only, meaning that a panel may find bad faith in circumstances not listed in the UDRP. The *Nuclear Marshmallows* decision, for example, concluded that passive warehousing could, in certain conditions, amount to bad faith registration and use.

Panel decisions have provided glosses on each of the circumstances listed in paragraph 4b.

Registration for the purpose of selling

Registration of a domain name for the purpose of selling it to the complainant, or to a competitor of the complainant would seem to cover the most straightforward instances of cybersquatting. The majority of panels have held that a general offer to sell the domain name is unequivocal evidence of bad faith. For example, in *General Motors Corporation v Vette Owners*,¹¹⁹ an advertisement offering to sell the disputed domain name <corvette.com> to 'anyone interested' was posted to the <corvette.com> Web-site. The panelist concluded that this was evidence that the domain name had been registered primarily for the purpose of selling it. Some panels, however, have held that a general offer to sell the domain name made some time after the name has been registered does not amount to evidence of registration in bad faith. *Id Software, Inc v Doom Gaming Connections*,¹²⁰ for instance, concerned the domain name <doom.com>. The respondent held the domain name for five years without developing the Web-site, then placed the name for sale on the auction site, e-bay.com. The panelist decided that there was no evidence that the domain name had been acquired for the purpose of selling it.

¹¹⁹ WIPO Case No D2000-0595 (October 20, 2000).

¹²⁰ NAF FA95002 (July 24, 2000).

An issue that has yet to be addressed by panel decisions is how the policy should treat unsolicited offers to buy the domain name followed, for example, by ‘without prejudice’ negotiations between the trade mark owner and the domain name registrant. In particular, as there is no international consensus on how to treat ‘without prejudice’ offers to sell, it is uncertain whether such offers will be admissible as evidence in UDRP proceedings.

Pattern of conduct to block registration of complainant’s mark

Panels have found that attempts to register large numbers of permutations of the complainant’s trade mark is evidence of bad faith. In *Magnum Piering, Inc v The Mudjackers*,¹²¹ the respondents registered domain names containing 14 variations of the complainant’s trade mark ‘MAGNUM PIERING’. The panelist held that registration of the names had no real purpose other than to prevent the complainant from reflecting its mark in a domain name. Similarly, previous UDRP and judicial decisions against the respondent may be evidence of an overall pattern of behaviour amounting to bad faith.¹²² On the other hand, merely registering a number of related domain names may not, by itself, amount to a pattern of behaviour. For example, in *Penguin Books Ltd v The Katz Family*,¹²³ the respondents registered the domain names <penguin.org>, <penguinland.org>, <penguinland.com> and <penguinland.net>. The panel held that the respondents had not engaged in a pattern of conduct and that there was no evidence that the domain names had been registered to prevent the complainant from reflecting its mark as a domain name.

Disrupting the business of a competitor

The third enumerated circumstance in paragraph 4b is interesting because, on its face, it has very little connection with protecting a complainant’s trade mark. This provision was apparently aimed at preventing the particular practice of a business competitor registering a domain name to block the trade mark owner from reflecting its mark in a domain name. Nevertheless, as expressed in the UDRP, the third circumstance is clearly much broader than this. There has been a degree of inconsistency in panel decision in relation to determining whether the domain name registrant is a competitor of the complainant. Most decisions have held that a respondent is a competitor only if it offers goods or services that compete with the goods or services of the complainant trade mark owner.¹²⁴ A minority of decisions, however, have held that a respondent that uses a Web-site to criticise a complainant is acting in opposition to the complainant, and is thereby a competitor.¹²⁵ This interpretation of the third listed circumstance would appear to be a serious mis-reading of the policy.

¹²¹ WIPO Case No D2000-1525 (January 29, 2001).

¹²² See, for example, *Nicole Kidman v Zuccarini* WIPO Case No D2000-1415 (January 23, 2001).

¹²³ WIPO Case No D2000-0204 (20 May 2000).

¹²⁴ See, for example, *Tribeca Film Center, Inc v Lorenzo Brusasco-Mackenzie* WIPO Case No D2000-1772 (April 10, 2001); *Compusa Management Co v Customized Computer Training* NAF FA95082 (August 27, 2000).

¹²⁵ See *Mission KwaSizabantu v Benjamin Rost* WIPO Case No D2000-0279 (June 7, 2000).

Confusion with complainant's mark

The fourth listed circumstance evidencing bad faith is clearly directed to activities that would give rise to traditional actions for trade mark infringement, or passing off. Using a confusingly similar domain name to attract Internet users in a way that dilutes the value of the complainant's trade mark is likely to amount to bad faith under this circumstance. For example, in *Universal City Studios, Inc v GAB Enterprises*,¹²⁶ the panel decided that using the domain name <fieldofdreams.com> to sell baseball merchandise diverted business from the complainant's site in a way that created a likelihood of confusion with the complainant's mark.

There has been some inconsistency in panel decisions dealing with the extent to which a disclaimer on the relevant Web-site may remove the likelihood of confusion. Some decisions have held that a prominent disclaimer of an association with the complainant precludes a finding of bad faith on the basis of a likelihood of confusion. For example, in *Al-Anon Family Group Headquarters, Inc v Don Reid*,¹²⁷ the panelist held that a conspicuous statement that the Web-site <al-anon.alateen.org> indicating that it was not the official Al-Anon/Alateen site was evidence of good faith use of the domain name. In *The New York Times Company v New York Internet Services*,¹²⁸ however, the panel decided that the inclusion of a disclaimer and a link to the authorised site was insufficient to dispel the initial confusion with the complainant's mark. In other words, the relevant time to assess the likelihood of confusion is the time of accessing the site, in which case a disclaimer is irrelevant as the user will not have had an opportunity to read it. On this analysis, it is the registration of a domain name that is similar to the complainant's mark that is likely to create confusion, rather than any use of the domain name.¹²⁹ This interpretation would appear to be at odds with the express words of the fourth enumerated circumstance.

9. Judicial Challenges to UDRP Decisions

Under Paragraph 4k of the UDRP, parties to a dispute are not prevented from submitting the dispute to a court of competent jurisdiction at any time before or after a panel decision. In other words, UDRP decisions are technically non-binding on the parties. An unsuccessful complainant may therefore bring an action at any time alleging, for example, that use of a domain name is trade mark infringement in the relevant jurisdiction, or pleading another cause of action, such as passing off. The position of an unsuccessful respondent is specifically dealt with in the UDRP. Paragraph 4k specifies that, following the decision of a UDRP panel that the domain name in issue will be cancelled or transferred, an unsuccessful respondent has ten business days in which to commence a legal action against the complainant. If ICANN does not receive

¹²⁶ WIPO Case No D2000-0416 (June 29, 2000).

¹²⁷ WIPO Case No D2000-0232 (June 5, 2000).

¹²⁸ WIPO Case No D2000-1072 (December 5, 2000).

¹²⁹ To like effect see *Estee Lauder Inc v Hanna* WIPO Case No D2000-0869 (September 25, 2000).

documentation evidencing that an action has been commenced within the ten day period, then it will implement the decision. If ICANN does receive relevant documentation, however, the panel decision will not be implemented until the matter has been resolved. The effect of legal proceedings initiated prior to, or during, a UDRP proceeding is set out at paragraph 18 of the *UDRP Rules*. Paragraph 18 provides that, in the event of legal proceedings, the panel has a discretion as to whether to suspend or terminate the UDRP proceeding, or to proceed to a decision.

Very few legal challenges to UDRP panel decisions have come before the courts.¹³⁰ Almost all challenges to UDRP decisions have been made under United States law. Trade mark owners that are a party to a UDRP dispute are in a unique position under United States law because of legislation that specifically deals with disputes between domain name registrants and trade mark owners, namely the *Anticybersquatting Consumer Protection Act*.¹³¹

9.1 Anticybersquatting Consumer Protection Act (ACPA)

The *ACPA*, which came into effect in late 1999, is specifically directed at protecting consumers and businesses against cybersquatting. It was enacted to remedy the perceived short-comings of United States trade mark law in dealing with cybersquatting. The *ACPA* establishes a new cause of action that is available against cybersquatters. Under the new action, a trade mark owner may bring an action against a person claiming both injunctive relief and damages if the following elements are made out:

- The defendant registers, traffics in or uses a domain name that:
 - in the case of a trade mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to the mark; or
 - in the case of a famous trade mark, is identical , or confusingly similar to, or dilutive of the mark; and
- The defendant has a bad faith intent to profit from the registered trade mark.

The *ACPA* provides the following non-exhaustive list of nine factors to be examined by the courts in determining whether a person has acted in bad faith:

- the trademark or other intellectual property rights of the person, if any, in the domain name;
- the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
- the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

¹³⁰ For a list of legal challenges of panel decisions see the WIPO Web-site at <http://arbiter.wipo.int/domains/challenge/index.html>. For a slightly more extensive list see: <http://www.udrplaw.net/UDRPappeals.htm>.

¹³¹ Codified as 15 USC s 1125(d) (1998).

- the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
- the person's intent to divert consumers from the mark owner's online location to a site that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark;
- the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used the domain name in the bona fide offering of any goods or services;
- the person's provision of material and misleading false contact information when applying for the registration of the domain name;
- the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others; and
- the extent to which the mark incorporated in the person's domain name is or is not distinctive and famous.

In addition to personal actions against a cybersquatter, the *ACPA* provides for trade mark owners to bring *in rem* claims directly against the domain name. The availability of an action *in rem* is designed to overcome the difficulties of proceeding against defendants who are difficult to locate or who are outside of the jurisdiction of United States' courts. An *in rem* action is, nevertheless, available only if the plaintiff can establish that it is not possible for the court to obtain personal jurisdiction over the defendant or that the plaintiff is unable, after 'due diligence', to locate the defendant.

There are obvious parallels between the cause of action established under the *ACPA* and the elements of abusive registration under the UDRP. This has led a number of panelists from the United States to adopt precedents established under the *ACPA* in interpreting the provisions of the UDRP. The different legislative histories of the two forms of dispute resolution, however, suggest that UDRP panelists should be cautious in applying precedents drawn from cases decided under the *ACPA*.

9.2 Challenges to UDRP decisions under United States law

Many of the cases in which UDRP decisions have been challenged before the United States' courts have involved narrow procedural issues. Some cases have, however, raised more substantive issues. This paper deals with two relatively recent decisions in which UDRP panel decisions have been challenged under the United States *ACPA*: *Jay D Sallen v Corinthians Licenciamentos*¹³² and *Barcelona.com, Inc v Excelentissimo Ayuntamiento de Barcelona*.¹³³

In *Corinthians*, the plaintiff had registered the domain name <corinthians.com>. The defendants, Corinthians Licenciamentos Ltda (CL), were the exclusive licensee of the 'CORINTHIAO' trade mark. 'Corinthiao' is Portuguese for 'Corinthians', the name of a popular Brazilian soccer team. CL filed a complaint under the UDRP with the WIPO

¹³² 273 F3d 14 (2001).

¹³³ United States District Court for the Eastern District of Virginia, Civil Action No 00-1412-A, 22 February 2002, available at <http://www.udrplaw.net/Barcelona.pdf>.

dispute resolution service. The WIPO panel decided that the domain name was confusingly similar to the 'CORINTHIAO' trade mark, that the domain name registrant had no rights or legitimate interests in the domain name and that the name had been registered primarily for the purpose of selling it to CL.¹³⁴ The panel ordered that the domain name be transferred to CL. Before the expiry of ten business days following the panel decision, the plaintiff filed a complaint in a United States federal district court, thus staying execution of the UDRP decision. The plaintiff sought a declaration that he was not in violation of the *ACPA* and a declaration that he was not required to transfer the domain name to the defendants. At first instance, the federal district court held that it could not order a declaration as there was no intention to sue the defendants under the *ACPA*. The decision was over-turned on appeal to the First Circuit Court of Appeals. The Court of Appeals held that the *ACPA* expressly provides a domain registrant that has lost a domain name under the UDRP with a cause of action for an injunction returning the domain name if the registrant can establish compliance with the *ACPA*. Furthermore, the Court of Appeals held that, in the event of a conflict between a UDRP decision and a decision under the *ACPA*, the *ACPA* decision would prevail. Given the similarities between the *ACPA* and the UDRP, the court held that a finding that a registrant was not a cybersquatter under the *ACPA* would necessarily negate a panel decision that the registrant was a cybersquatter under the UDRP. The Court of Appeals therefore remanded the case to the federal district court for a decision under the *ACPA*.

The weight to be accorded to a UDRP panel decision in making a determination under the *ACPA* came before the United States District Court for the Eastern District of Virginia in the *Barcelona.com* case. In that case, the plaintiff sought a declaration that registration and use of the domain name was not unlawful under the *ACPA*. The defendants, the city government of Barcelona, had previously been successful in establishing abusive registration under the UDRP.¹³⁵ The court decided that, given that UDRP proceedings are non-binding and that United States legislation required no deference to UDRP decisions, no weight whatsoever should be given to UDRP decisions in proceedings under the *ACPA*. On the substantive issues, the court refused to grant a declaration and found that there had been a breach of the *ACPA*. The court therefore confirmed the UDRP panel decision and ordered the transfer of the domain name to the city of Barcelona.

10. Dispute resolution in the .au namespace

The development of policies relating to dispute resolution in ccTLDs is the responsibility for the authorities administering the ccTLD. The .au Domain Administration Ltd (auDA) is responsible for developing and administering policies in relation to the .au ccTLD. In June 2001, the auDa Dispute Resolution Working Group presented a report to the auDA board recommending the adoption of a dispute resolution policy, to be known as the

¹³⁴ *Corinthians Licenciamentos LTDA v Sallen* WIPO Case No D2000-0461 (July 17, 2000).

¹³⁵ *Excelentísimo Ayuntamiento de Barcelona v Barcelona.com Inc* WIPO Case No D2000-0505 (August 4, 2000).

auDRP.¹³⁶ The proposed auDRP is modelled on the UDRP, but includes a number of modifications. The auDRP modifications are largely intended to take into account the extent to which registrations in 2LDs under the .au ccTLD are subject to policy restrictions, unlike registrations in the open gTLDs to which the UDRP applies.

A number of further modifications to the UDRP have, however, been incorporated as a result of experience with the UDRP. In particular, there are two important modifications in relation to what amounts to abusive registration. First, the auDRP effectively incorporates the *Nuclear Marshmallows* decision by providing that a complainant need only establish that a domain has been registered *or* subsequently used in bad faith.¹³⁷ While this change appears to do no more than codify decisions made under the UDRP, it may well result in the auDRP applying to a greater range of disputes. Second, the auDRP modifies the first of the non-exclusive circumstances evidencing bad faith. Under the UDRP, the first of the listed 'bad faith' circumstances refers to registration of the domain name for the purpose of selling it to the complainant or a competitor of the complainant. The auDRP has modified the wording of this example of bad faith so that it applies to registration for the purpose of selling the domain name to 'another person'. Given that UDRP panels have commonly decided that general offers to sell the disputed domain name amount to bad faith, this may not represent a significant change. On the other hand, it may mean that attempts to auction a domain name are more likely to be considered as evidence of bad faith.

The recommendations of the auDA Dispute Resolution Working Group have been accepted by the auDA board and the auDRP is scheduled to be introduced in conjunction with the new competitive registry system during the first half of 2002. Nevertheless, existing domain name licences will be 'grandfathered', meaning that registrants who licensed their domain name before introduction of the auDRP will not be subject to the auDRP unless they choose to 'sign on' to the auDRP. Upon renewing their domain name, however, registrants will be required to agree to submit to the auDRP as part of their domain name licence agreement.

11. Conclusion

Legal protection of commercial indicia, such as trade marks, has conventionally focussed on preventing persons other than the owners from using the indicia in ways likely to create confusion in relation to the source of goods or services offered by the trade mark owner. More recently, there has been a tendency for legal protection to extend to protecting the investment in a mark against uses likely to dilute the value of the mark to the trade mark owner. Registration of domain names that are similar to commercial indicia, such as trade marks, creates difficulties for conventional legal principles. For example, a domain name may not necessarily be used in relation to goods or services.

¹³⁶ auDA Dispute Resolution Working Group, *Proposed .au Dispute Resolution Policy (auDRP) and Rules*, June 2001, available at <http://www.auda.org.au/docs/auda-audrp-final.html>.

¹³⁷ auDRP, paragraph 4a.

Nevertheless, it could be argued that, given the increasing economic and social importance of the Internet, mere registration of a domain name that is similar to a trade mark may, in itself, be thought to create confusion, or at least some harm to the trade mark owner. On the other hand, as each domain name is unique, every person with an interest in a trade mark cannot be entitled to register the identical mark as a domain name. Moreover, those without an interest in a mark sufficient to amount to ownership of an intellectual property right, might be thought to have an entitlement to have this interest reflected in a domain name. For example, people interested in criticising the owner of a commercial indicia might be thought to be entitled to register a domain name that reflected this interest in the indicia. Given these considerations, it would seem that trade mark owners cannot possibly be entitled to prevent the registration of all possible permutations of the mark as domain names. Something more than mere registration of a domain name that is similar to a trade mark would seem to be required for there to be a trade mark infringement, or for the elements of an action such as passing off to be satisfied. The courts have, nevertheless, struggled to identify the additional requirements necessary for registration of a domain name to be unlawful under traditional legal forms of protection of commercial indicia. Particular difficulties have been experienced in the application of traditional legal principles to cybersquatting and related practices, which involve attempts to use the registration of a domain name that is similar to a trade mark in an attempt to extract some payment from the trade mark owner, or to otherwise profit at the expense of the trade mark owner. Although, under Anglo-Australian law, the tort of passing off has proved flexible, there are considerable areas of uncertainty in relation to its application to cybersquatting and related practices. In particular, difficulties may be encountered in identifying the relevant misrepresentation associated with the registration of a mark as a domain name.

The difficulties of adapting traditional forms of legal protection to cybersquatting, together with the costs and practical problems of bringing actions against cybersquatters, led to the development of a new form of dispute resolution specifically directed at cybersquatting and related practices. The ICANN UDRP was designed to be an informal, quick and inexpensive means for resolving disputes between trade mark owners and domain name registrants. In practice, UDRP panels have dealt with a remarkably large number of disputes within a relatively short period of time. Nevertheless, UDRP decisions have been subject to considerable criticism from academics and other commentators. In particular, critics have been concerned with the degree of inconsistency between panel decisions dealing with similar matters, and with the extent to which panel decisions have appeared to extend protection of real world indicia beyond that originally intended.

There are a number of explanations for the level of inconsistency apparent in UDRP panel decisions. First, there is a degree of ambiguity concerning the extent to which the policy is aimed at cybersquatting and the extent to which it is aimed at preventing trade mark infringement. Second, there is some uncertainty concerning the use of precedents derived from national legal systems in panel decisions. This can sometimes result in a rather mechanical application of principles developed in the context of domestic trade mark law to a quite different context. Third, there is a lack of institutional checks on

panel decisions, including no internal appeals mechanism. Fourth, a considerable number of panel decisions are made without the respondent filing a reply.

The relatively large number of default decisions is also likely to be a factor in explaining the extension of the policy beyond that apparently originally envisaged. Moreover, the considerable discretion given to panels under the UDRP deriving, for example, from the general wording of the elements of abusive registration and of the non-exclusive examples of bad faith, appears to have encouraged some panelists to interpret the policy broadly. The informal and experimental nature of the process may also have played some role. On the whole, however, it would appear preferable for panelists to confine themselves to applying the policy, rather than creating policy.

Although the number of disputes dealt with under the UDRP, and the relatively few legal challenges to UDRP decisions, represents an important achievement, it seems clear that steps can be taken to improve the quality and consistency of panel decisions. Some reforms that could be considered include:

- Establishment of an internal appeals mechanism, especially from single person panel decisions. This would establish an incentive for panels to be more rigorous in their decisions and provide redress in the case of the few especially egregious decisions.
- Examine mechanisms for reducing the number of default decisions. For example, steps could be examined for providing information to respondents to assist in lodging a reply.
- Clarify the choice of law rules under the policy, so that relatively arbitrary application of national legal principles can be avoided.
- Monitor the extent to which ccTLD dispute resolution systems diverge from the UDRP.