Domain Names, the UDRP and Cybersquatting – A short note on shortcomings of the UDRP and a suggested remedy to deter Cybersquatters

Abhishek Singh

Abhishek Singh is a final year law student at Sydney University.

Introduction

Since its adoption, the Internet Corporation for Assigned Names and Numbers' (**ICANN**) Uniform Domain Name Dispute Resolution Policy (**UDRP**) has proved an effective tool for resolving cybersquatting disputes. Yet, critique has been levelled at the providers of dispute resolution under the UDRP for being inherently biased towards trademark owners, that such bias is eroding the rights of fair use,[1] and that despite its successes, cybersquatting is still on the rise.[2]

This article argues that an 'architectural change' in the software and hardware of the system that enables domain name registrations, might be an indirect method of curbing the incidence of cybersquatting.

The UDRP: Aims and Objects

The UDRP's objective was to combat the cybersquatting problem. Cyber squatting involves persons registering domain names reflective of, mostly well known, trademarks for unfair commercial purposes, such as selling the domain name to the trademark owner at inflated prices. This was the case in *British Telecommunications Plc v One in a Million Ltd and Ors*[3] (BT) where the defendants registered numerous domain names reflective of famous trademarks, including **www.bt.org**[4].

The UDRP seeks to provide trademark owners with a fast and reliable way to settle cybersquatting disputes by appointing panelists who decide whether:

(a) the registered domain name is confusingly similar to the complainant's trademark;[5]

(b) the registrant has no legitimate rights or interests in the domain name;[6] and

(c) the domain name was registered in bad faith.[7]

This is also known as the 'cybersquatting test'.

Where all these requirements are satisfied, the panelists generally hold the trademark owner entitled to the domain name reflective of the trademark, and order that the domain name be transferred to them or cancelled. The cost of such panel decisions is paltry compared to litigation.[8]

The Problem

While the UDRP can be effective at solving cybersquatting disputes, the problem is that due to a number of factors, the UDRP policy is frequently misapplied. Indeed, it has been argued quite convincingly that the fundamental reason for such misapplication is an erroneous interpretation of the scope of trademark law.[9] The following cases illustrate the bases for such an argument.

In *Bayer Aktiengesellschaft v Dangos & Partners,*[10] the respondent registered **www.bayersucks.org** and there was evidence to suggest a pattern of 'abusive' domain name registrations, in that the domain names registered by the respondent were usually linked to sites offering to sell that particular domain name. Essentially, the cybersquatting test was satisfied.

The point is this: although the WIPO panel acknowledged that domain names like www.bayersucks.org could be used to voice public critique, the panel went on to state that:

"...as long as the Respondent owns the disputed domain names, it will be beyond the complainants [i.e. Bayer's] control to prevent such use of the domain names...the respondent will have the ability to tarnish the Bayer mark..."[11]

This is unsatisfactory, because the panel seems to accept that Bayer is, by way of its ownership of the trademark, entitled to control the disputed domain names. This is arguably an incorrect conception of trademarks, the primary purpose of which is to reduce customer search time by helping them distinguish particular products from others in the same market. While ownership of a trademark does give the owner the exclusive right to associate the mark with the owner's product or service, it should not give the owner the right to control the voicing of opinions about the mark or the company the mark is owned by.

In an earlier case, *Telstra Corp Ltd v Nuclear Marshmallows,*[12] the panel accepted 'non-use' of the domain name **www.telstra.org** as evidence of a bad faith registration. The reasoning was that the registration itself, which prevented Telstra from gaining access to the domain name, amounted to bad faith given how well known the Telstra name was. Such reasoning clearly disregarded the language of the UDRP, which specifically requires that the domain name be registered and used in bad faith, before a cybersqatting case can be made out.[13] It is fair to say that cybersquatting by a competitor of the trademark owner can amount to 'use' of the domain name, but registration by others who wish to criticize the domain name ought not to.

Notwithstanding the above, the UDRP is clearly useful in resolving cases such as BT, where the registrant actively 'speculated' in domain names, or the case of *Panavision Int'l L.P. v Toeppen,*[14] where the defendant coupled offers to sell to the plaintiff a domain name identical to Panavision's trademark with promises not to register other domain names that were 'deceptively similar' to the Panavision mark. The court found traditional trademark infringement. Yet another instance of the usefulness of the UDRP is an arbitration case where the Princeton Review registered **www.kaplan.com** in order to attract the customers of its competitor, Kaplan, in the standardized test preparation materials market.[15]

All the Wrong Incentives

As of August 2003, 7324 UDRP cases had been determined; complainants prevailing in nearly 5802 of these cases, or nearly 80% of the time.[16] Complainants generally prevail because many UDRP decisions are straightforward cases involving plain instances of cyber squatting. Yet, 556 proceedings are currently pending as of August 2003.[17] While some may be what are called 'Reverse Domain Name Hijacking'[18] cases, Armon argues convincingly that this increase in domain name disputes is partly explainable by structural deficiencies in the UDRP policy.[19] Armon's argument is simple: given the cost of a having a single panelist decide a UDRP case ranges between US$750-1500, and more for three panelist decisions, a rational complainant would be willing to pay up to US$1500 for a domain name as opposed to going through the UDRP. In such situations, the registrant stands to make the difference between their registration fee for the domain name, and what a complainant pays for the domain name.

So on the one hand, the UDRP provides an effective cybersquatting solution, whilst paradoxically providing an incentive for cybersquatting. While numerous reforms have been proposed to the UDRP structure, such as appeal processes,[20] these are changes that deal with the resolution of disputes, and not with the causes for their occurrence.

One way to see such proposals is through the eyes of Lawrence Lessig, who posits that there are four regulators of individual behavior in democratic society, namely: law, the market, social norms and architecture.[21]

'Architecture' in the sense Lessig uses it, refers to the design of things and how that defines the limits of human action, whether in real or cyber space. 'Law', in the context of domain name disputes, refers to the UDRP, as that is effectively the law that parties to domain name disputes submit to. The important point is that in cyberspace, architecture and how systems are designed can dictate what can and cannot happen to a greater extent than in real space. Architecture can be a better regulator than law in cyberspace.

Thus, changing the rules and regulations of the UDRP amounts to changing law in order to directly effect changes in behavior, namely, curbing the incidence of cybersquatting. However, changing the architecture of domain name registrations may be a better way of achieving the same objective.

Convincing Trademark owners to be less paranoid and dissuading cyber-squatters from squatting; irreconcilable goals or a job for architecture?

Domain name registrations are generally carried out online and the current software simply registers the requested domain name so long as no one else has an identical domain name. Thus, A could register **www.mooncheese.com** and B could register **www.moncheese.com**. More relevantly, A could register **www.toshiba.com** so long as Toshiba Ltd Japan has not registered the domain name; no authentication is required to register so long as the relevant fees are paid. The only warning given is that the registrant may be liable for registering domain names that violate the rights or interests of others.[22]

Thus, it is arguable that cybersquatting is enabled by virtue of the architecture which enables domain name registrations allowing for it.

What is proposed instead is a more sophisticated system as follows:

ICANN could change the architecture (i.e. make the necessary software and hardware changes) of domain name registrations so as to effect two changes:

(a) Establish a link between domain name servers and the equivalent of a series of locally registered trademarks root servers, which would contain a comprehensive list of locally registered trademarks, the list being updated regularly in real time.

(b) Creating a new top level domain (**TLD**) devoted to 'fair use' such as the proposed '.sucks' domain name.[23] This TLD could then be implemented at state level, e.g. '.sucks.au'.

These proposals could work in the following manner:

When a new registrant asked for a domain name, the domain name registration server could require the registrant to disclose what the purpose of using the registration is and who the target audience is, e.g. the new registrant states that the domain name will be used to retail shoes in Australia. Based on such information, the registration server would communicate with local trademark servers in Australia to compare the requested domain name and the list of uploaded locally registered trademarks in respect of shoes, or shoe stores. This comparison could incorporate a level of comparative sophistication, in that the comparative component of the domain name registration software would incorporate algorithms that compare the requested domain name with registered trademarks to check for confusing similarities between the two.

If the requested domain name is similar, such as **www.reebokrules.com**, then a window could pop up, informing the potential registrant of the confusing similarity. The potential registrant would then have two options – they could be redirected to the 'fair use' TLD to register their domain name or they could proceed to register the domain name if they are able to attach a digital certificate or a digital copy of a certificate from the relevant trademark owner that authorises them to register the requested domain name. ICANN could reserve the right to cancel the registration if the digital certificate proves to be unauthorised or fake. Such authentication could take place by way of the registration taking effect only upon verification of the authenticity of the digital certificate with the relevant trademark owner. This could be accomplished by way of e-mail communications between ICANN and the trademark owner. In this way, local trademark owners get to control domain names so as to prevent use that may infringe their trade mark or be used in bad faith, while 'fair use' registrants can continue to register domain names. The attraction of such a system lies in the fact that it allows trademark owners to control non-infringing use of their trademarks without significantly expanding their legal rights. Of course, the owners of globally recognized trademarks will be able to get adequate protections provided they have the requisite local registrations in place.

How will this help?

The above changes are no doubt ambitious, I do not purport to be aware of all the technical issues they raise; but I do believe that they would actively dissuade cybersquatting, whilst at the same time balancing the rights of trademark owners with those of free speech and voicing opinions. Two shortcomings in the above proposal are, first, unscrupulous persons may resort to registering domain names under the fair use domain for trademark violation purposes. An example would be Mr. A registering **www.compaq.sucks** to sell fake Compaq computers, in which case the UDRP could be changed accordingly to deal with such cases. Secondly, registrants may be able to circumvent such a system by lying about the intended use and target audiences, but it is hoped that the proposed use of digital certificates would dissuade such practices.

Conclusions

The UDRP policy has arguably been the first effective step in the regulation of conduct online. Its operation since 1999 has made the Internet and business community aware of the UDRP's shortcomings and strengths. Putting in place a system of domain name registration similar to that proposed along with complementary changes to the UDRP may encourage the migration of commerce to cyberspace. This may come about by reducing the opportunities for domain name registrations in bad faith; and by striking a more even balance between the rights of trademark owners and fair use registrants. In putting forward these proposals, I do not purport to have chanced upon a panacea. Rather, the proposals should be seen as different in that they posit indirect changes to architecture and not direct changes to the UDRP itself as a means of dissuading the very real problem of cybersquatting.

[1] See generally: Geist M, "Fair.com? An Examination of the Allegations of Systematic Unfairness in the ICANN UDRP", available at: www.udrpinfo.com/resc/fair.pdf

[2] See: Armon O, "Is this as good as it gets? An Appraisal of ICANN's Domain Name Dispute Resolution Policy (UDRP) Three Years after Implementation", (2002) 22 *Rev. Litig* 99 at 137

[3] [1999] FSR 1; [1998] 4 All ER 476; [1999] 1 WLR 903

[4] Other plaintiffs in the BT case were Virgin Enterprises Ltd, J.Sainsbury Plc, Marks & Spencer Plc and Ladbroke Group Plc, to name a few.

[5] ICANN UDRP Art 4 (a) (i)

[6] ICANN UDRP Art 4 (a) (ii)

[7] ICANN UDRP Art 4 (a) (iii)

[8] The two main providers of UDRP dispute resolution services, WIPO and the National Arbitration Forum (NAF) charge between US$750-1500 per case where a single panelist is appointed, and more for cases where 3 panelists are requested – See: Geist M, note 1 at 3-4

[9] See generally: Goldstein A, "ICANNsucks.biz (and why you cant say that): How Fair Use of Trademarks in Domain Names is being Restricted", (2002) 12 *Fordham Intell. Prop. Media & Ent. L.J.* 1151 at 1158; Geist M, note 1 above.

[10] WIPO Case No. D2002–1115, available at: http://arbiter.wipo.int/domains/decisions/html/2002/d2002-1115.html

WIPO Case No. D2002–1115, available at: http://arbiter.wipo.int/domains/decisions/html/2002/d2002-1115.html decision of Angelica Lodigiani, Sole Panelist, Dated 3 February 2000

[12] WIPO Case No. D2000-0003, available at: http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0003.html

[13] UDRP Art 4 (a) (iii)

[14] (1998) 141 F.3d 1316 (9th Cir), and for a discussion of the case see: Goldstein A, note 9 at 1160

[15] Goldstein A, note 9 at 1160, FN41, citing David Yan, "Virtual Reality: Can We Ride Trademark Law to Surf Cyberspace?" (2000) 10 *Fordham Intell. Prop, Media & Ent. L.J.* 773 at 777

[16] Statistical Summary of Proceedings under the Uniform Domain Name Dispute Resolution Policy, available at: http://www.icann.org/udrp/proceedings-stat.htm

[17] Statistical Summary of Proceedings under the Uniform Domain Name Dispute Resolution Policy, available at: http://www.icann.org/udrp/proceedings-stat.htm

[18] Term used to describe situations where complainants attempt to use the UDRP procedures to deprive a registrant of a domain name in bad faith. For a detailed discussion see: Hollander J, "The Impact of Reverse Domain Name Hijacking", available at: http://www.gigalaw.com/articles/2002-all/hollander-2002-03-all.html

[19] Armon O, note 2 at 137

[20] Geist M, note 1; Davis G, "The ICANN Domain Name Dispute Resolution Policy, The UDRP in Perspective after Nearly Two Years of History", available at: http://www.isoc.org/oti/printversions/1201icann.html

[21] See Generally: Lessig L, *Code and Other Laws of Cyberspace,* (USA: Basic Books, 1999), Ch 7: What Things Regulate

[22] This is the wording of the UDRP, Art 2(b), it is safe to assume that it forms a part of the terms of the online contract between the relevant domain name registrar and the registrant

[23] Goldstein A, note 9 at 1181, FN150