E-commerce

Commission building capacity with slam-a-cyberscam

Consumers have more opportunities to protect themselves and others against scams in cyberspace after the Commission's upgrade of its slam-a-cyberscam webpages.

Slam-a-cyberscam is an automated service able to take thousands of complaints at a time about illegal online selling practices. As occurs for other types of conduct the Commission may respond to a complaint made online with enforcement action. But slam-a-cyberscam also helps the Commission to process complaints data efficiently, to identify emerging problems in electronic commerce and to deal with them swiftly.

The service can be accessed through the Commission's website at <http://www.accc.gov.au>.

Since its launch in April 2001 slam-a-cyberscam has taken more than 70 complaints including allegations of illegal conduct.

The Commission will continue to expand its capacity to deal with the increasingly electronic nature of commerce and conduct in Australia.

Domain name submission

The following is an edited version of the Commission's submission to the second Public Consultation Report of the auDA Name Policy Advisory Panel.

The Commission welcomes the opportunity to submit its views on the panel's public consultation report on allocation policies and eligibility criteria for the Australian segment of the Internet Domain Name System (DNS). The Commission applauds the panel's efforts in revising the policies and maintaining a high degree of integrity within the system, while catering to the special needs of its users.

The Commission makes the following comments in its capacity as a regulator of electronic addressing, including the DNS, in Australia. The Commission has powers under Division 3 of Part 22 of the *Telecommunications Act 1997* as amended by the *Telecommunications Legislation Amendment (Electronic Addressing) Act 2000*. These powers include making recommendations to the Australian Communications Authority (ACA) for it to declare a manager of electronic addressing. Once such a declaration is made for a person or association, the Commission may issue directions to them on electronic addressing matters affecting competition and consumer protection.

The Commission supports the bulk of the recommendations in the report. It commends the panel for focusing on practices that may result in dampening uptake of the Internet as an alternative way to communicate, conduct business and disseminate information. It supports the panel's goal in making the system as conducive to automation as possible and in relaxing the current policies where appropriate. It welcomes the panel's willingness to look at new ways of freeing up the .au DNS through the addition of new 2LDs (second level domains) and the possibility of making generic and geographic names available.

Registration of products and services and application of trademark law

The Commission notes the advantages of having a hierarchy of purpose-driven 2LDs, and of having rules that can be applied consistently. It has been argued that this structure is the reason there have been far fewer disputes over rights to names in the .au domain than in other less restricted domains — particularly the generic top level domains (gTLD). The criteria

to ensure that the integrity of the system is maintained have also generally allowed applications to be treated consistently. The Commission sees consistency as a key to providing certainty to the users and therefore confidence in the DNS, and the Internet as a whole.

Another factor in providing confidence in the DNS is the degree of certainty users have in their ability to retain their chosen domain name. On this point the Commission notes the recommendations that trademarks be included as a criterion for eligibility for a name (rec. 3.1.3d), and that a domain name simply have a connection to the registrant instead of being derived from the name of the registrant (rec. 4.1.1). This represents a fundamental shift from the way domain names are presently registered. Under these recommendations it will now be possible for product names or services and other activities to be identified by a domain name.

The report also recommends that applicants acknowledge that their entitlement to a domain name may be challenged by a third party with superior legal rights in the words forming the domain name (rec. 3.1.3f). The Commission would be concerned if the application of these recommendations, either singly or in combination, led to the unjustified precedence of trademark or other intellectual property rights over the existing rights of licence holders, as this may raise issues of market power and consumer protection under the Trade Practices Act.

The Commission is unaware of any law or legal ruling that suggests one right is superior to another in this area. In the absence of guidance provided by such instruments, it would be appropriate for the panel to consider the nature of domain names and trademarks separately before attempting to weigh the relative rights of one against the other. It is not apparent from the report that the panel has done this.

Proceeding on this assumption, s. 17 of the *Trade Marks Act 1995* (TMA) defines a trademark to be a sign used, or intended to be used, to distinguish goods or services provided in the course of trade by one person from the goods and services so provided by another person. Domain names are user-friendly masks for Internet protocol (IP) numbers. IP numbers are used to identify the physical location of computers connected to the Internet — in short, they act as addresses, although domain names may represent secondary benefit to their holders as a means of marketing and branding.

The rights conferred by registration of a trademark include exclusive use of the sign, the right to authorise other persons to use the sign, and to obtain relief for infringement of the sign (s. 20 TMA). Registration of a trademark also confers personal property rights (s. 21 TMA). Domain names are not property (according to one US court ruling) but are for conditional use by the registrant under a limited licence from the authority for the DNS, in this case auDA.

Under the limited examination above, it is apparent that domain names are a way to distinguish one computer from another, and not to distinguish the goods and services of competing businesses. It would therefore appear the DNS is not substitutable for the trademark system.

The question of the degree to which the opportunity for marketing and branding from a domain name is affected by trademark law is complex and unresolved, so attempting through this forum to attribute trademark rights to Internet addresses may be premature. Trying to extend the trademark system into the DNS may therefore result in unintended and unforeseen conflict with other law, as well as the practical consequence of potentially dampening demand for participation in, and provision of, online services.

Should users, for whatever reason, believe trademarks confer superior rights to a domain name, then the Commission remains concerned that there may be a rise in disputes and a trend in domain names accruing to larger businesses. This accrual may occur because smaller parties generally lack the resources to fight the matter through the alternative dispute resolution process or further, or because the entire process may be slanted towards registrants who have trademarks. This is likely to be exacerbated by the recommendation that applications for trademarks be accepted as the basis for registrations (rec. 4.1.2), even though such applications may later be rejected by the Registrar of Trademarks.

The Commission notes that the present registration system has resulted in some persons registering company and business names solely for the purpose of registering a domain name. The Commission agrees that this results in poor allocative and productive efficiencies for the administrators of corporations law and for the registrants themselves. It should be noted, however, that expanding the eligibility criteria to include applications for trademarks may also lead to some persons applying for trademarks for purposes unrelated to the goods and services they provide. These purposes may include establishing bona fides for the use of a domain name — whether legitimate or not, protection of an existing domain name, or prevention of others from registering the name. As such, eligibility criteria based on trademarks by themselves will not necessarily lead to improvements in market conduct, falling costs, or improvements in the integrity of the DNS.

Additionally, allowing the registration of products and services potentially creates inconsistencies with some other recommendations that should be resolved before presentation to the auDA board. The retention of the system of purpose-driven 2LDs is based partly on making the DNS easy to use for all Australians. Allowing domain names to be based on products and services as well as registrants' names may make it harder for people who use intuitive navigation to reach the address they are seeking. Similarly, the inclusion of products and services may unnecessarily complicate the administration of other allocation rules such as those relating to generic and geographic names, particularly if other 2LDs should be introduced that cover these types of domain names.

Also, the purposes of the various 2LDs as they currently stand are predicated on names being derived from the name of the registrant. The proposed change will require review of the wording of each purpose if consistency across all policies is to be retained.

Finally, allowing registration of products and services as domain names may pre-empt consideration of what new 2LDs might be created in the future. auDA has already extended the NPAP's (name policy advisory panel's) terms of reference to include consideration of how and what new 2LDs might be introduced. One potential 2LD would be one that caters for products and/or services. However, the proposed recommendations may effectively obviate the need for such a 2LD, but would do so without the necessary consideration that would be given to the proposal if it was made in accordance with the extended terms of reference.

The Commission supports the recommendations that allow registered trademarks to be used to satisfy eligibility criteria only to the extent that the trademark applies to the name of the registrant, and to the extent that the trademarked name acts to distinguish the goods and services of the registrant from those of its competitors.

The Commission does not support the recommendations that allow products and services to be registered as domain names within the same 2LD as entity names.

Consistency and retrospectivity

The Commission continues to receive complaints that a small percentage of individual applications have been processed in contravention of the current policies. One complainant provided a list of more than 1300 registered domain names that appear to be inconsistent with existing guidelines. Complainants generally are concerned about the disadvantage they suffer by comparison with the licensees of these domain names. The more evidence there is that policies are applied inconsistently, the greater the loss of confidence in the registration system. The Commission understands that the policies have been changed over the years, and that this is part of the reason for the apparent inconsistency. However, this is small comfort to those parties who feel aggrieved by it.

If the recommendations of the report are adopted by auDA, then there will be a further layer of inconsistency in the types of names that have been registered. The Commission notes the preference of some parties for maintaining the existing rights of existing licence holders, but draws the panel's attention to the requirement for licence holders to satisfy the eligibility criteria at the time of licence renewal (rec. 3.1.2). This might provide a viable means of removing inconsistency of policy application in a staged way, which will allow affected parties to plan and manage the change.

The Commission recognises that enforcing retrospectivity will be affected by various factors. These would include additional cost to affected parties, the windfall advantage gained by the parties, and the effect of perceived inconsistency in policy application on penetration of business and other users into the online environment.

The Commission therefore reserves its opinion on whether the report's recommendations should or should not be applied retrospectively, but notes that without retrospectivity, consistency of policy application is unlikely. It is therefore unlikely that without retrospectivity the system will encourage the level of user confidence that would otherwise be possible. The Commission suggests that auDA monitor this issue, irrespective of its final decision, and revisit it as part of any future review of its domain name policies.

Alternative dispute resolution

In view of the concerns outlined above, consideration should be given to how a future alternative dispute resolution mechanism may be evenly balanced in its treatment of the competing rights of those who use it. The report proposes that a uniform dispute resolution policy (UDRP) implemented by auDA apply to 2LDs only on an opt-in basis (rec. 6.2.1). The Commission questions the effectiveness of such a process if not all parties are bound by it. The danger may exist that some parties that would be subject to complaint or dispute may use the opt-in clause to avoid resolution of those disputes except by costly legal means.

The Commission suggests that an opt-out alternative dispute resolution process would give greater comfort to the Internet community. Under this arrangement, all parties would be subject to a UDRP unless auDA had made an individual exemption on specific grounds that it might choose to develop.

Proposed pricing structures

The Commission notes the report's comments on the cost implications associated with a derivation rule (rec. 4.1.2a and 4.1.2b). In general, and unless it has a legislative responsibility for price setting, the Commission's view is that a regulatory body should not make recommendations on pricing structures, or otherwise unnecessarily influence the pricing decisions of firms in a competitive market. The Commission sees the level of fees charged by registrars for registering domain names under different derivation rules as a matter for those registrars based solely on their own cost structures and business plan.

Submission to WIPO on domain name registration

The following is an edited version of the Commission's submission to the World Intellectual Property Organisation's (WIPO's) 2nd Public Consultation on Domain Name Registration.

The Commission welcomes the opportunity to comment on these draft recommendations.

The Commission has specific regulatory powers in relation to the administration of domain name policy in Australia, and has been an active participant in recent work on domain name policy and industry structure carried out at the request of auDA, the administrator of the .au domain space. As a statutory regulatory agency the Commission acts at 'arm's length' from the Australian Government, and while it has consulted widely within the Australian Government and with auDA in preparing this submission, it should not be seen as an Australian Government submission.

The Commission supports and applauds WIPO's willingness to further the work begun in the 1st Public Consultation Process to resolve problems of disputes between parties claiming the right to use domain names. In particular, the Commission supports the methodology adopted by WIPO in defining the issues, scoping the extent of any problems, and identifying the range of options available to resolve the perceived problems.

Moreover, the Commission endorses the following five key principles specified by the interim report that respect should be had for:

a) the diversity of purposes that the Internet is used for;

b) the limitations of existing law and the proposition that new law should only be effected through representative and legitimate authority;

c) agreed rights outside the sphere of intellectual property;

d) the functionality of the Internet in not making recommendations that impose an unreasonable burden on its operation; and

e) the underlying dynamic nature of the technology in not making recommendations that condition or affect the future technological direction of the Internet.

The Commission considers that WIPO's intent to use these principles to determine its final recommendations as being crucial to the success of the process, the continued health of the Internet and its ability to benefit people all over the world.

In the context of its roles and responsibilities, and in view of its belief in the aptness of the stated principles, the Commission offers the following comments.

Overview

It is apparent from the interim report and from submissions to the earlier requests for comment that there are two distinct problems being experienced by users of the generic top level domains (gTLD) of the domain name system (DNS). These are bad faith registrations (cybersquatting) and competing legitimate claims to a domain name. Irrespective of the type of identifier, whether it be trademark names, any of the categories identified in the interim report, or some other identifier, a complainant will either allege that a domain name licence holder has no claim to the name or that their own claim is stronger.

Currently, the success of such a claim relies only on the protection conferred by one or more of the various internationally agreed treaties in relation to trademarks, the way that protection has been defined by the uniform dispute resolution policy (UDRP), and the way that an arbitration panel interprets the applicability of the UDRP to the claim.

However, the legal basis for granting protection against bad faith registration is uncertain. Intellectual property appears to be the 'best fit' to some observers, but extending intellectual property law into the DNS may have some unintended and detrimental effects on its users, and on the competitive process generally.

This submission proposes that further consideration be given to:

- tightening the registration process so that cybersquatting is harder to engage in;
- using the UDRP to remove existing cases of cybersquatting;
- expanding the DNS so it more closely resembles the reality of the offline world, so that users can distinguish where a particular entity may reside in the DNS, and so that the existing framework of laws may be applied more easily than at present;
- limiting the use of the UDRP to dealing with bad faith registrations, since, in the absence of harmonised legislation specifically developed for the protection against cybersquatting, or suitable amendments to the UDRP, it may not be appropriate for use in determining competing legitimate claims to a name; and
- requiring accurate Whois information as a way to increase user confidence in the Internet (Whois is an Internet directory service used for looking up names of people on a remote server).

Cybersquatting

For the purposes of this submission, the Commission accepts the present definition of cybersquatting as being the bad faith registration of a domain name, and the UDRP definition of bad faith registration as having no rights or legitimate interest in the name in dispute. Currently, the UDRP is only available to trademark owners.

The terms of reference for the 2nd consultation process seek to expand the definition of cybersquatting to include registrations that are abusive, misleading or unfair, and to apply the definition in relation to other types of identifiers as well as trademarks. The Commission agrees that the definition requires expansion because the harm resulting from cybersquatting is not

confined to trademark holders. In revising the definition, it should be noted that other laws will be applicable including competition law, fair trading law, privacy law and the declaration of human rights.

Under trade practices law, abusive, misleading and unfair practices have particular connotations. Misleading conduct generally refers to conduct that causes consumers to make decisions based on false or incomplete information, and often implies the use of deception to bring this about. Unfair conduct is a generic term that may be applied to consumer protection as above, otherwise known as fair trading; to conduct that has a detrimental impact on the competitive process; or to conduct that is considered unconscionable. Under Australian law the definition of unfair competitive conduct is normally linked to a misuse of market power, or predatory purpose. Similarly abusive registration may be applied to situations of 'reverse' cybersquatting for which the registration may be linked to an abuse of market power. Bad faith registrations may have the effect of any or all of the types of conduct described here.

However, abusive registrations could also conceivably include registrations that do not raise consumer protection or competition issues. Domain names such as those in the form of 'entitysux.suffix' are clearly an expression of free speech, and may serve pro-consumer protection and competition purposes by encouraging 'entity' to improve its service levels. WIPO needs to ensure that the definition of cybersquatting in its final report does not inadvertently capture legitimate, if possibly distasteful, registrations.

The harm from cybersquatting

The Commission is concerned that the practice of cybersquatting may restrict competition and confuse consumers about the nature and content associated with a particular domain name. There are four elements to assessing the ill-effect of bad faith registration. These are the extent of the problem, the loss suffered by the 'victim', the unintended harm caused by the response to it, the impact on user confidence in the DNS and subsequent effects flowing into the wider community.

The interim report notes there are over 35 million registered domain names of which over 21 million are in the .com gTLD. The UDRP has been used to render over 3640 decisions in just over 15 months.[1] On the face of it, this represents fewer than 0.02 per cent of domain names that have been subject to dispute so far. Against this, no mention is made of the number of disputes pending or resolved outside the UDRP. Anecdotal evidence suggests that the names of prominent companies such as Telstra and Nissan have been included in hundreds of domain names or more. Moreover, since the UDRP is limited to use by trademark holders only, a more fitting comparison would be the number of disputes as a proportion of domain names attracting trademark rights.

Even if there is only a small percentage of names that are subject to dispute, there may still be significant loss involved on the part of the 'victim'. This loss may be in the form of money paid to cybersquatters to recover the name, amounts paid to register a dispute and to pursue the dispute to its conclusion, and in notional amounts for cost of capital and opportunity cost. Other forms of loss may be in the reputation of the claimant, in market share through being unable to have a presence on the Internet that can leverage off the entity's good name, and in loss of trade in cases where the cybersquatter engages in passing off. In cases where personal names have been cybersquatted, there may also be loss of personal standing and quality of life.

Sums that have been quoted for recovering a domain name are frequently in the tens of thousands, but are reported to be in the millions for some names. The cost of notifying a dispute under the UDRP is US$1500, but there are other direct costs to a claimant in progressing a dispute that may add tens of thousands of dollars in legal representation, research and lost productivity. Similarly, with sums of this nature there are opportunity costs and costs associated with employing capital in this way, which may also run into the thousands. It is much harder to quantify losses in trade and marketshare,

1 Interim report para. 4.

but these may also be significant. Finally, it is impossible to place a figure on the loss of goodwill, or personal reputation, but these are areas that should not be underestimated.

As was noted in WIPO's first consultation process, there is a danger that trademark holders, irrespective of whether the mark is registered or covered by common law, may gain an unwarranted advantage in applying for and retaining their domain name of choice.[2] This can arise in various ways. First, the assumption that a domain name attracts trademark protection creates and reinforces the perception that a domain name actually is a trademark. Second, trademark holders may, and some would argue do, exploit this perception by claiming trademark rights in every domain space to the detriment of other users with legitimate claims to the same or similar names. Third, UDRP panellists, in trying to enforce the spirit of the mechanism, may further reinforce the perception through hearing claims that may fall outside the scope of the wording of the UDRP, or they may simply misinterpret its aim. Then, of course, there is the problem of controversial or wrong decisions.

The final factor to note in assessing the harm from cybersquatting is the flow-on effect to the Internet and the wider community. The losses mentioned above will ultimately be passed on to consumers, so it is not just the claimants that suffer this loss: it is the entire community. As WIPO's consultation processes show, there is strong interest from groups of Internet users in protecting the DNS from cybersquatting activity. Increasingly, there are greater numbers of domain name resellers who base their services on fear of cybersquatters and the need to protect names from unscrupulous individuals. This can lead to entities registering their name, and its variations in multiple domains, including those where the opportunity for bad faith registrations is much more limited than in the open gTLDs. One consequence of this can be congestion of the DNS, and increased difficulty for other users in obtaining their domain name of choice.

Also, as incidents of cybersquatting are reported, and responded to, the reputation of the Internet suffers as potential and actual users receive the perception that the Internet is largely uncontrolled and the haunt of unethical characters. This can lead to a loss in confidence in the medium. This can result in fewer online transactions, fewer users willing to interact online, fewer domain names being registered, and less competition and innovation in online services.

It is therefore apparent that the extent of both the loss from cybersquatting and the wider effects are likely to be out of all proportion to the number of domain names that are subject to bad faith registration. For these reasons the Commission proposes that consideration be given to prohibiting cybersquatting irrespective of the type of identifier that is affected. The means of doing this is discussed later in the paper.

The proposal of a prohibition on cybersquatting raises the difficult question of whether there needs to be a legal basis for such a prohibition, and what that might be.

The legal basis for protection against cybersquatting

The Commission believes that WIPO, ICANN (Internet Corporation for Assigned Names and Numbers) and other authoritative bodies must ask some basic questions about the nature of domain names before settling on measures that may have quasi-legal status in the minds of those using the DNS. The interim report notes that the Internet should not be subject to different application of existing law than the offline world, or to different layers of regulation. To ensure this does not occur it is important to keep in mind what the DNS does and what a domain name is.

2 *The management of Internet names and addresses: intellectual property issues*, available at <http://wipo2.wipo.int/process1/report/finalreport.html>.

The DNS functions as the address system for the Internet, allowing connectivity between computers by identifying the location of content hosting servers. Domain names are the visible labels for these locations. A domain name consists of two separate elements: the discretionary string chosen by the registrant; and the hierarchical suffix that distinguishes where the string will sit within the DNS.

A domain name licence holder will have no rights in the suffix, as this is part of the DNS hierarchy, although it may have rights in the offline world associated with the string. Therefore, consideration should be given to whether a domain name, as the physical address associated with an online entity, merits the status of a trademark, particularly when a physical address in the offline world, such as a phone number or street address may not qualify for registration as a mark. Similarly, a domain name may not qualify for protection under other laws simply because the string may be protected under those laws in the offline world.

The interim report and several submissions note that rights do not attach to a name per se, but are infringed according to the use that a name is put to.[3] In the offline world for instance, it is only relevant that an entity is passing off, not that it is doing it from a particular street address, or using a particular telephone number. Similarly, in the online world the domain name is only the location where the activity in question is occurring. According to this view no action would be taken in relation to the street address or phone number. By extension of the principle that online law should be the same as offline law, then no action should be taken in relation to a domain name.

However, a domain name is often the only identifier that a cybersquatter uses. Also, some aspects of bad faith registration depend entirely on the domain name itself. If the Whois information is deficient, and the cybersquatter cannot be located, then the only protection against the cybersquatter is to take the domain name away. In the absence of anti-cybersquatting law, the legal basis for terminating the licence for a domain name must then be either contractual, or rooted in an existing law that is not purpose built, but which may only be a 'best fit'.

Problems with existing mechanisms

WIPO's first effort in recommending the UDRP shows the effectiveness of a contractual approach. Mandating the UDRP as a precondition of domain name registration extends the application of the trademark system to protect trademark holders wanting to develop an online presence. The interim report proposes that the UDRP now be amended in a number of different ways to cater for the specific types of protection offered by treaties such as the Paris Convention and the TRIPS Agreement to different types of identifiers.[4] However, as the five key principles enunciated in the interim report specify, respect must be had for:

a) the diversity of purposes that the Internet is used for;

b) the limitations of existing law and the proposition that new law should only be effected through representative and legitimate authority;

c) agreed rights outside the sphere of intellectual property;

d) the functionality of the Internet in not making recommendations that impose an unreasonable burden on its operation; and

e) the underlying dynamic nature of the technology in not making recommendations that condition or affect the future technological direction of the Internet.

The UDRP in its present form does not meet all of these objectives completely, and cannot protect entities other than trademark holders that also desire to have an Internet presence. The intellectual property system may be used to underpin a decision to transfer or cancel a domain name that may be claimed to infringe a trademark, but it cannot be used to guarantee an individual the choice of the domain name —

3 For example: Interim report paragraphs 40, 49, 95, 146, 153–4, 203–4, and 288.

4 Interim report recommendations at paragraphs 57 (INNs), 115 (IGOs), 227 (geographical indicators and indications of source), 278 (country and administrative region names), and para. 322 (trade names).

unless the individual can represent themself as a commercial enterprise. Some other means must be found to give legitimacy to their fight against cybersquatting.

The interim report proposes several different solutions to the single problem of cybersquatting depending on the type of protection that an identifier enjoys in the real world.[5] This will mean making some amendments to the UDRP to cater for the different types of protection to be afforded to the different types of identifier. Multiple changes of this nature to the UDRP will increase the factors that panellists must take into account. This will also increase the complexity and cost of administration of the UDRP.

The Commission considers that further thought and emphasis should be given to dispute prevention, rather than sole reliance on the UDRP to address cybersquatting. Disputes will continue unless the registration process is tightened in ways that address the factors that make cybersquatting possible. It is recognised that dispute prevention mechanisms will increase the cost of registration, but these are likely to be more than offset by the savings resulting from removing the harm from cybersquatting identified in this submission.

The interim report acknowledges that the UDRP, in either its present form or as amended by the draft recommendations, may be used to decide issues that are more appropriately dealt with in courts of law.[6] This represents a significant danger to the DNS and the Internet as a whole. This issue is considered in greater detail in the section on 'Competing rights'.

For all of the above reasons the Commission suggests the following approach should be considered as a possible solution.

Prohibition on cybersquatting

It is suggested that WIPO recommend to ICANN that it consider taking steps to impose a blanket prohibition on bad faith registration in all gTLDs and ccTLDs (country code top-level domains).

A measure such as this would require a definition of what constitutes 'bad faith' registration, a way to restrict people's ability to make bad faith registrations in the future, a way to redress bad faith registrations made in the past, and a dispute resolution process if rejected registrations are challenged.

Definition of bad faith registration

It is considered that a workable definition of 'bad faith' is already contained in the ICANN UDRP, and would require only minor amendment. At present the UDRP is applicable to entities defined under paragraph 4a. Under this proposal, references that equate domain names with trademarks should be amended to reflect the degree to which rights apply to the string. Similarly, if words such as 'trademark' and 'service mark' are used, they would be replaced by a more generic term such as 'mark' or 'name'.

Controlling bad faith registrations

Currently, the UDRP is applied as part of the contract between the registrar and the registrant. Restricting the number of bad faith registrations may be achieved through the same contract by requiring registrants to produce proof of a legitimate interest in a domain name. Proof of a continuing legitimate interest would also be required as part of the domain name licence renewal process. This requirement to develop rules for gTLDs is likely to clash with the existing aims of the gTLD registrars, which is to maximise the number of registrations.

5 For example, paragraph 83 recommends an exclusion mechanism for INNs, paragraph 123 recommends that exact matches for IGOs be prohibited from registration in all but the .int domain, paragraph 186 calls for submissions on changes to the UDRP to protect personal names, paragraph 227 recommends that the UDRP be expanded to cover geographic names in the new gTLDs, paragraph 275 recommends that registration ISO 3166 country codes be prohibited in the new gTLDs, while paragraph 322 recommends that trade names receive no protection.

6 Paragraphs 18, 56, 129, 137, 166, 168, 177, 312–314, 320.

In answer to this it should be noted that in the offline world many countries require registration of a company or business name before trading is legally allowed to commence. There are also significant penalties for providing false information in the registration process. In the online world, registration of a domain name is a practical requirement before trading can begin. However, there are no similar penalties for providing incorrect or inaccurate details. Introduction of a system such as this at the gTLD level would do away with much of the need for exclusions, reserved lists or other technical additions to the DNS. This does not mean that a reserved list approach is not appropriate for names such as INNs (international nonproprietary names) that may not be registered as a trademark or other identifier in the offline world. A precedent for this approach in the online world is contained in auDA's recent approval of the recommendations of the *Names policy advisory panel final report* available at <http://www.auda>.

It should also be noted that while it may be more difficult to introduce these measures in the existing open gTLDs, this is not so for proposed new domains recently announced by ICANN. The opportunity exists to ensure that the cybersquatting problem cannot take hold in these domains as it has in others that have no pre-registration requirements.

Retrospective action on bad faith registrations

Existing bad faith registrations may be dealt with under the UDRP as amended above. Given that bad faith registration may contravene various laws, a decision under the UDRP should not be seen as being the end of a matter. Contraventions of competition law, defamation law or passing off law carry substantial penalties in many jurisdictions. It may therefore be inappropriate for the only penalty to be the loss of a domain name. In these circumstances, a requirement to refer a matter to the relevant law enforcement authority may be warranted.

A requirement such as this would have the added advantage of increasing the risk for bad faith registrants. Increasing the risk makes the practice much less attractive in the first place. If cybersquatting is less lucrative, then the problem may be controlled much quicker than if the penalty remains insignificant.

The Commission believes that a UDRP that is aimed at eradicating bad faith registrations should be adopted by all ccTLD administrators. Without this step its effectiveness will be undermined by different expectations and levels of understanding between complainants and respondents with names in different domains.

Appeal against decision not to register

One consequence of introducing criteria into the registration process is that some registrations will be disallowed. There is an increased risk that registrars will make mistakes in disallowing some registrations. It is accepted practice in most administrative decision-making processes that there be an avenue of appeal. When a decision to reject a registration on grounds of bad faith is challenged, the UDRP could be extended, or a separate process established to deal with these. Consequently, an appeal process would need to be established that can consider whether the criteria that have been introduced to the registration process have been applied fairly and correctly.

Competing rights

The interim report contemplates the difficulty of reaching agreement on the protection to be accorded to different identifiers under different international treaties and law. The submissions to WIPO's RFC-2 (WIPO's second request for comment) show there are diverse views on the identifiers. In particular, the discussion on trade names, personal names and geographical indicators indicate a multiplicity of rights that affect the operation of the law in the offline world.

The interim report also recognises that there are serious doubts about the competence of the existing UDRP panels to make decisions that necessarily interpret international law and the application of international treaties for disputes between two or more legitimate claims to the same domain name.[7] It is possible that an arbitration mechanism could satisfactorily

7 Paragraphs 129, 168, 320.

resolve these questions provided that the mechanism accords with the principles of a viable legal system. These include those included in the New York Convention on the Registration and Enforcement of Foreign Arbitral Awards, 1958. In accordance with the key interim reports principle 'b' (which requires respect for the limitations of existing law and the proposition that new law should only be effected through representative and legitimate authority), and until such time as the UDRP can meet the principles espoused by the New York convention, the Commission believes that the UDRP should be limited to resolving questions of bad faith registration.

The Commission is keen to see that any administrative or judicial process developed to resolve conflicting claims for domain names deliver an appropriate balance between the protection of intellectual property and other rights while not affecting the competitive process within the DNS or the wider Internet, or the operation of consumer protection laws.

An approach that unduly favours the rights of intellectual property rights holders may restrict competitive access to domain names. Equally an approach that does not sufficiently protect legitimate intellectual property rights may raise 'free-riding' issues. Key factors to be considered in resolving this issue include:

- clarification of the degree to which intellectual property rights extend to domain names;
- the role of other laws including competition law;
- the appropriate forum for disputes between competing rights;
- the impact of introducing new domains; and
- the impact of limiting the number of domains in which a string may be registered.

Notwithstanding this view, it is possible to reduce the frequency that disputes may arise by revising the structure of the DNS, and requiring domains to serve a particular and unique class of domain name, as was one of the original intentions. For instance, the .com gTLD should be required to register only names of commercial enterprises. Similarly, gTLDs that serve other individual classes of name would not be able to register names that are not in that class. For instance, a motor car company should not be able to register its name or products as a .pro name, since that domain is for professions.

Even if opposition to such a scheme renders it unworkable in the established open gTLDs, the idea should still be considered for those new domains that have yet to begin operation.

Such an approach may also assist domain name licence holders in differentiating their products and services online. Arguments put forward that the only domain of value is the .com domain may prove to be short term, and highlight the difficulty of leveraging off the strength of a brand name in the offline world. As people become more familiar with the DNS and the Internet generally, they will realise that there are far more locations than just .com. The opportunity will then exist for entities to leverage off the values encapsulated by domains that maintain distinctiveness. It needs to be noted that a successful online presence will still be dependent on traditional offline measures such as advertising to bring that presence to the notice of customers, although domains that have strict eligibility requirements can help in locating individual entities.

The lack of distinguishing features within the open gTLDs also impedes the viability of the DNS for effective and user-friendly Internet navigation. Consider the example of a commercial enterprise wishing to register its trading name as part of a .com domain name. However, an individual with the same or similar name may have registered it first. The enterprise must then select a different gTLD or ccTLD in which to register. Users trying to locate the company will now have to play a guessing game to find the correct domain that the enterprise chose. The devaluation of the domain space becomes more apparent if the individual has no commercial activity associated with the registered .com domain name.

The frequency of disputes could also be lessened by further partitioning of the domain name space through the creation of additional gTLDs and lower level domains for particular communities of interest. The DNS is a virtual system and so it is expandable to a virtually unlimited degree. As the interim report suggests, a new domain could be created for IGOs

(international intergovernmental organisations),[8] and we suggest for INNs. Alternatively, IGOs could be included with other entities qualifying for inclusion in the .int domain. Providing that registration in the new domains is appropriately controlled, the risk of cybersquatting and other disputes can be minimised. Similar approaches may be adopted for geographic names, trademark names and other identifiers that are not well served by the existing hierarchy of domains.

A further issue in dispute prevention is whether there should be limitations on the number of TLDs in which entities are able to register a particular string. For example, an entity has registered xyz.org, and then applies for xyz.org.au and xyz.org.nz. The Commission's view is that if disputes are to be kept to a minimum, and as many users as possible are to have access to the DNS, then entities should only be able to do this in limited and controlled circumstances. In determining what those circumstances may be, the earlier comments on the importance of advertising should be noted. Also, commercial requirements to cater for specific customer segments can be satisfied by technical means such as load sharing between servers. Instead of having multiple domain names, a firm could have one global domain name that points to servers in different locations to satisfy the requirements of different customers.

Views suggesting that a string attracting intellectual property or other rights should be able to exercise those rights in every domain need to be assessed very carefully. For example, when a company lists in a telephone directory, users are not misled because there are multiple parties with the same or similar names. Nor do the different parties that share a common name suffer loss from the co-listing. Similarly, a company that has a premium toll-free phone number has no right to claim that number for its facsimile service, its fixed telephone service, its mobile telephone service, or any other numbered service it may want to operate.

Moreover, trademarks provide protection only in the country in which they are registered, and not across international borders.

Until the legal question of the degree to which intellectual property and other rights apply to domain names is settled, the Commission advocates that WIPO continue its present emphasis on the five key principles, particularly respect for the diverse uses of the Internet.

The Commission suggests that further consideration of how to reduce the disputes between parties that each have legitimate claims to a domain name should be the subject of a third (or more if required) public consultation process to consider the issues outlined above in more detail.

The Commission does not support any call to have these disputes resolved through the UDRP or any such administrative mechanism, until such time as the proposed mechanism is capable of effectively addressing all the factors relevant to such disputes.

'Whois' information

The Commission is one of many agencies that have a particular interest in the integrity of Whois information. The interim report recommends that all registrars be required to collect and maintain accurate Whois data. As the report notes, this data is essential for identifying the holders of domain names. Complainants under the UDRP need this information to know who their claim should be made against, and panellists to know who to notify of claims against them. Accurate Whois information is pertinent to this consultation process.

There are two other significant reasons why registrars should be required to ensure the integrity of this data. Consumers who may be considering an online purchase, or who may have a dispute about an online transaction need to know who to contact, and how to contact the trader. Not all websites provide this information, so an alternative way is needed for consumers to be able to approach online sellers.

8 Paragraph 112.

The second reason is to allow law enforcement agencies to be able to identify the persons responsible for domain names that have been used for activity that may be in breach of the law. In the absence of accurate domain name information, many illegal activities will go unchecked for the simple reason that it has been impossible to identify and locate the offender.

The Commission proposes that accurate Whois information be collected and maintained through the contract between registrars and registrants. The registrant should be required to notify the registrar of any changes to contact details as and when they occur. The discovery of inaccurate information should be grounds for termination of the contract and the cancellation of the domain name, once the domain name holder has had a reasonable opportunity to correct the errors.

Conclusion

The Commission believes that the suggestions contained in this submission, if adopted, would meet the objective of enhancing the welfare of all Internet users by promoting competition and fair trading in the DNS and catering for consumer protection in the way the DNS is administered.