WORLD INTELLECTUAL PROPERTY ORGANIZATION

世界知识产权组织

ORGANIZACION MUNDIAL DE LA PROPIEDAD INTELECTUAL

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE

المنظمة العالمية للملكية الفكرية

ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

March 18, 2005

Dear Dr. Cerf,
Dear Mr. Twomey,

./. Further to your request, I have pleasure in attaching to this letter a document addressing intellectual property issues involved in the introduction of new generic Top-Level Domains (gTLDs).

The document is based on insights gained through previous consultative processes organized by the World Intellectual Property Organization (WIPO), and WIPO's experience in the implementation and administration of procedures aimed at curbing abusive practices in the domain name system, including the Uniform Domain Name Dispute Resolution Policy (UDRP) and the various intellectual property protection mechanisms developed by some operators of previously introduced new gTLDs.

/...

Dr. Vinton G. Cerf
Chairman
Mr. Paul Twomey
President and CEO
Internet Corporation for Assigned
Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601
United States of America

By post and email: vinton.g.cerf@mci.com
twomey@icann.org

cc: Mr. Mohamed Sharil Tarmizi
Chair
ICANN Governmental Advisory Committee

By email: sharil@cmc.gov.my

I hope that you will find this document helpful in developing and implementing a comprehensive strategy for introducing new gTLDs. WIPO remains available to collaborate with ICANN in the establishment of balanced and effective intellectual property protection mechanisms for new gTLDs.

On a different matter, I hope that, since no opposition was voiced in the public forum on the Recommendations made by the Member States of WIPO in the context of the Second WIPO Internet Domain Name Process (the "WIPO-2 Recommendations"), work on implementing these Recommendations can now begin. We shall be delighted to cooperate with you in this matter.

With best regards,

Yours sincerely,

Francis Gurry
Deputy Director General

WIPO ARBITRATION AND MEDIATION CENTER

New Generic Top-Level Domains: Intellectual Property Considerations

World Intellectual Property Organization

Overview

1. Background

1. This report responds to a request made by Paul Twomey, the President and CEO of the Internet Corporation for Assigned Names and Numbers (ICANN) with letter dated April 27, 2004. In this letter, Mr. Twomey requested the World Intellectual Property Organization (WIPO) to provide expert advice on "intellectual property issues involved in the introduction of new gTLDs".

2. The request is based on the following resolution passed by the ICANN Board of Directors on October 31, 2003:[1]

> "Whereas the development of an appropriate process and policy for the creation of new gTLDs has been a topic of Board and community debate since the creation of ICANN.
>
> "Whereas there is a fundamental need for a comprehensive process to move from the proof of concept test commenced with the 2000 round to the liberalization of the gTLD market.
>
> "Whereas ICANN needs to deliver this comprehensive approach to new gtlds not only in response to community demand, but also toward completion of a task agreed under ICANN's new MoU with the U.S. Department of Commerce.
>
> "Whereas ICANN has committed to deliver, by September 2004, a comprehensive evaluation of:
>
> (a) The potential impact of new gtlds on the Internet root server system and Internet stability;
> (b) The creation and implementation of selection criteria for new and existing TLD registries, including public explanation of the process, selection criteria, and the rationale for selection decisions;
> (c) Potential consumer benefits/costs associated with establishing a competitive environment for TLD registries; and
> (d) Recommendations from expert advisory panels, bodies, agencies, or organizations regarding economic, competition, trademark, and intellectual property issues.
>
> "Whereas ICANN is also committed to define and implement a predictable strategy for selecting new gtlds using straightforward, transparent, and objective procedures that preserve the stability of the Internet (development of strategy is to be completed by September 30, 2004 and implementation to commence by December 31, 2004).
>
> [...]

---

[1] The full text of the resolution is available at *http://www.icann.org/announcements/advisory-31oct03.htm*.

"Whereas expert advice is expected to be sought from areas including:

- an international economics organization on the introduction of competition into the TLD market and other similar markets, allocation mechanisms and possible appropriate business models for the TLD manager-ICANN relationship;
- a review and report on intellectual property issues involved in the introduction of new gtlds to be provided by the World Intellectual Property Organization;
- consumer protection issues, potentially from a consumer protection agency;
- reports from the Internet Architecture Board and ICANN's Security and Stability Committee on technical stability issues related to the introduction of new gtlds, including planning for registry failures;
- assessment of the Internet Architecture Board on the need for additional technical standards to support multilingual TLDs."

3. The present document provides the requested advice. It is based on insights gained through previous consultative processes organized by WIPO, and WIPO's experience in the implementation and administration of procedures aimed at curbing abusive practices in the domain name system (DNS). This includes the experience gained in the context of the first expansion of the generic domain name space which began on November 14, 2000 when the ICANN Board of Directors selected a first group of new gTLDs: .aero, .biz, .coop, .info, .museum, .name, and .pro.

4. Because of the limitations inherent in ICANN's mandate, the document does not deal with country code Top-Level Domain Names (ccTLDs), although many of its findings may also be relevant in that context. Moreover, the document is limited intellectual property (IP) issues that are of direct relevance in the context of the creation of new gTLDs and does not address other IP issues, such as issues relating to Internet content. The document does not deal with other policy matters that may be relevant for the creation of new gTLDs. As already stated in the Final Report of the First WIPO Internet Domain Name Process:[2]

> "311. [...] in view of the variety of issues and perspectives involved in the formation of a policy on the creation of new gTLDs, it goes without saying that the intellectual property perspective is not the only one to be taken into account. In considering the formulation of recommendations concerning the addition of new gTLDs, therefore, the approach has been adopted of assessing what the past experience of intellectual property owners has been in relation to problems encountered in the current gTLDs, and using that experience as a basis for recommending how the particular interests of intellectual

[2] The Management of Internet Names and Addresses: Intellectual Property Issues. Final Report of the First WIPO Internet Domain Name Process ("First WIPO Report"), WIPO Publication No. 439, also available at *http://arbiter.wipo.int/processes/process1*.

property owners can be accommodated within an overall policy on the creation of new gTLDs."

5. Hence, this document does not discuss the question as to whether new gTLDs should be introduced at all. Many IP owners have voiced their concern about, or opposition to, the introduction of new gTLDs because they fear that any further expansion of the domain name space will provide additional room for abusive domain name registrations. While it could be argued that, from an IP perspective, the best way to protect IP rights may consist in refraining from introducing additional gTLDs, it is recognized that IP issues, while important, are not the only policy issues to be taken into account when deciding on the introduction of further gTLDs. Moreover, the manner in which such introduction could or should take place will only be considered where it is relevant for IP protection.

6. After summarizing the main IP concerns raised by new gTLDs, the document will, first, provide an overview of the relevant recommendations made by WIPO thus far. A separate chapter will examine the efficiency of the Uniform Domain Name Dispute Resolution Policy (UDRP) in providing relief against, and preventing, the abusive registration and use of domain names, and whether the introduction of new gTLDs has led to an increase in cybersquatting. The document will then analyze, on the basis of the experience of the WIPO Arbitration and Mediation Center ("WIPO Center"), the efficiency of the various IP protection mechanisms designed by some new gTLD operators. The final part will consider when preventive IP protection mechanisms are necessary, and provide a comparative overview of various such mechanisms.

2. Domain Names and Intellectual Property

7. In addition to their technical function as Internet addresses, domain names have assumed further significance as identifiers. As stated in the First WIPO Report:

> "10. [...] As commercial activities have increased on the Internet, domain names have become part of the standard communication apparatus used by businesses to identify themselves, their products and their activities. Advertisements appearing in the media now routinely include a domain name address, along with other means of identification and communication, such as the corporate name, trademark and telephone and facsimile numbers. But, whereas the telephone and facsimile numbers consist of an anonymous string of numbers without any other significance, the domain name, because of its purpose of being easy to remember and to identify, often carries an additional significance which is connected with the name or mark of a business or its product or services."

8. This additional significance has brought the DNS in contact, and in conflict, with the traditional systems of identifiers that existed before the Internet. These identifiers are mostly protected by closely regulated systems of IP rights which aim to preserve the orderly functioning of markets through the avoidance of confusion and deception.

2.1 Domain Names and Trademarks

9. So far, IP protection in the DNS has focused on trademarks, a specific category of identifiers which serve to distinguish the goods or services of one company from those of another. As stated in the First WIPO Report:

> "11. [...] A trademark enables consumers to identify the source of a product, to link the product with its manufacturer in widely distributed markets. The exclusive right to the use of the mark, which may be of indefinite duration, enables the owner to prevent others from misleading consumers into wrongly associating products with an enterprise from which they do not originate."

10. Trademarks serve as a focus for the goodwill associated with a product as a result of investments in quality and marketing. Brand recognition through trademarks enables start-up companies to establish a successful business presence and more established brands to preserve their reputation and value. For a growing number of companies in developed and developing countries, trademarks have become the single most important business asset, their value often exceeding that of such companies' physical assets.

2.2 Domain Names and Other Identifiers

11. Other protected identifiers include trade names, personal names,[3] geographical indications, International Nonproprietary Names (INNs) for pharmaceutical substances and the names and acronyms of international organizations (IGOs). Such identifiers have also become the subject of abusive practices in the DNS. To develop recommendations on means of dealing with such abuse, WIPO conducted the Second WIPO Internet Domain Name Process. The Second WIPO Report was published in September 2001 and discussed by the Member States of WIPO, who in September 2002 recommended to provide protection for country names and for the names and acronyms of IGOs in the UDRP. These recommendations (the "WIPO-2 Recommendations") were transmitted to ICANN in February 2003 and continue to be under ICANN's consideration.[4]

---

[3] Personal names are strictly speaking not considered to be IP rights, but may enjoy a similar degree of protection under national laws, see The Recognition of Rights and the Use of Names in the Internet Domain Name System. Report of the Second WIPO Internet Domain Name Process ("Second WIPO Report"), WIPO Publication No. 843, paragraphs 169-204. Also available at *http://arbiter.wipo.int/processes/process2*.

[4] Cf. the "WIPO Briefing Note on the Second WIPO Internet Domain Name Process" posted at *http://www.icann.org/tlds/stld-apps-19mar04/stld-public-comments.htm*.

2.3 Intellectual Property Concerns

12. Given the value of trademarks and other identifiers and the importance of the Internet as a commercial communication and marketing channel, rights owners are understandably worried that their identifiers fall victim to deceptive and abusive practices on the Internet. Undermining the status of such identifiers also compromises the credibility of the DNS and consumers' trust in the Internet as a medium for commercial exchange. The First WIPO Report found that:

> "315. [...] the priority concern of the trademark community does not relate to conflicts between parties who claim to have competing legitimate rights in the name (for example, different companies with the same trademark in different product lines or operating in different areas of the world), but focuses on cases of clear abuse, often directed at famous and well-known marks."

13. Such concerns are based on previous experience with abusive practices in the existing open gTLDs where domain name registrations are granted purely on a "first come first served" basis. Such abuses have forced trademark owners to invest substantial human and financial resources in defending their interests. The damage that a trademark owner suffers as a result of the abusive registration and use of a domain name may well be extensive by virtue of the global accessibility of domain names. The First WIPO Report notes in this regard:

> "132. [...] A considerable disjunction exists between, on the one hand, the cost of obtaining a domain name registration, which is relatively cheap, and, on the other hand, the economic value of the damage that can be done as a result of such a registration and the cost to the intellectual property owner of remedying the situation through litigation, which may be slow and very expensive in some countries."

14. IP owners therefore often adopt a preventive approach by registering their most valuable identifiers (sometimes including misleading variations) in all relevant gTLDs in order to preempt abuse. Such defensive registrations cause substantial cost both for the registration of domain names as well as for the maintenance of large domain name portfolios.[5]

---

[5] See OECD, "Generic Top Level Domain Names: Market Development and Allocation Issues", July 13, 2004 ("OECD Report"), *http://www.oecd.org/dataoecd/56/34/32996948.pdf* at page 34: "The strongest argument for not creating new domain names is the cost to business users of defensive registrations. It is difficult to quantify what this might be but some of the major elements can be specified. The cost of a single registration under a gTLD, with prices starting as low as 4.95 United States dollars per annum, is unlikely to be the major consideration for business users. It is true that many businesses register multiple domains and this may be a consideration depending on the number they want to register. More likely, however, the largest cost consideration for business users is the administrative and legal costs of managing an increased portfolio of domain names. In some cases this may be substantial."

3. Intellectual Property and New gTLDs

3.1 Benefits for IP Owners?

15. It is sometimes argued that the introduction of new gTLDs may actually benefit IP owners, for example by enabling them to obtain gTLDs that reflect their trademarks, or by providing greater space for brand differentiation.

16. *IP-gTLDs.* The possibility of obtaining a gTLD that is clearly associated to their identifier may well be attractive to rights owners. However, such a possibility risks importing to the top level conflicts that already exist on the "second level", i.e. conflicts between domain names and IP rights. Such conflicts may occur (i) between rights owners and abusive applicants who acquire the gTLD with a view to exploit the goodwill associated with that identifier, and (ii) between competing rights owners. The potential for conflicts will further increase with the introduction of "internationalized" TLDs which open additional possibilities for registering confusingly similar variations of identifiers.[6]

17. The procedure for attributing new gTLDs would therefore have to be designed in a way that avoids such conflicts as much as possible. In this respect, some lessons may be drawn from the experience gained with "Sunrise" mechanisms[7] which raise similar issues albeit on a different level (the top level instead of the second level). As a minimum, the right to use the identifier should be verified before the gTLD is assigned. As with Sunrise mechanisms, it could be considered to limit the possibility of acquiring a gTLD to owners of marks that are famous or well known across a widespread geographical area because such marks enjoy a higher level of (international) protection.[8] It may also be advisable to enable competing rights owners to intervene in the attribution procedure. This could facilitate the resolution of disputes before a new gTLD is assigned and avoid burdensome subsequent litigation. In addition, further safeguards may be necessary, such as a requirement that the right on which the application is based was acquired before a certain deadline in order to prevent speculators from acquiring rights merely for the purpose of obtaining a particular gTLD.

18. *Brand Differentiation.* Thematic differentiation in the DNS, or within a gTLD, may, at least in theory, allow targeting domain name registrations to specific purposes and user groups, and enable owners of identical or similar trademarks that are used for different goods or services ("United" for courier services and "United" for air transport services) to obtain domain names that reflect their trademarks in distinct subject matter gTLDs.

---

6 This experience has already been made with "internationalized domain names" (IDNs) which offer additional possibilities of registering domain names that are confusingly similar to a protected identifier, see the WIPO Briefing Paper prepared for the Joint ITU/WIPO Symposium on Multilingual Domain Names, December 6 and 7, 2001, "Internationalized Domain Names - Intellectual Property Considerations", available at *http://arbiter.wipo.int/domains/internationalized/index.html*.

7 Sunrise mechanisms are analyzed in more detail below at paragraphs 124-137.

8 See paragraph 30 below.

19. However, such differentiation works only when gTLDs are restricted to limited and clearly circumscribed specific purposes. The less this is the case, the less will further gTLDs enhance the possibilities for differentiation. This is true, in particular, for the following three types of gTLDs:

(i) completely unrestricted gTLDs, such as .info;

(ii) gTLDs with minimal or nominal restrictions such as .biz, which is open for any "*bona fide* business or commercial use";

(iii) gTLDs with geographic rather than subject matter restrictions, such as the proposed new sponsored gTLD .asia for the "Pan-Asia and Asia Pacific community".[9]

20. When one trademark owner registers its trademark in one such gTLD and another owner registers an identical or similar mark in another gTLD, the public will not be able to clearly attribute each domain name to a specific trademark owner without checking the web site content (unless perhaps if one mark is clearly much more famous than the other). This is likely to cause confusion. Moreover, to the extent Internet users are unable (or become unaccustomed) to associate one mark with a specific business origin, the distinctive character of a trademark will be diluted.

21. As a result, trademark owners are likely to try to register their marks in all such gTLDs. Indeed, a recent report commissioned by ICANN suggests that those new gTLDs that had either no (.info) or only minimal registration restrictions (.biz), had the lowest number of new domain name registrants and the largest share of registrants that already held over 100 domain names.[10] This suggests that a large number of domain names was registered for defensive purposes. Hence, from an IP perspective, adding more open, i.e., unrestricted and unsponsored gTLDs, is more likely increase the likelihood of confusion (and the cost for defensive or preemptive measures) than the scope for brand differentiation.

3.2 Curative and Preventive IP Protection Mechanisms

22. Given previous experience, it is likely that the opening of a new "empty" domain name space will attract abusive registrations of valuable "real estate". There are essentially two ways of providing protection:

---

9 See the .asia New sTLD RFP Application, *http://www.icann.org/tlds/stld-apps-19mar04/asia.htm.*

10 Summit Strategies International, Evaluation of New gTLDs: Policy and Legal Issues, July 10, 2004 ("New gTLDs Report"), page 100, *http://icann.org/tlds/new-gtld-eval-31aug04.pdf.*

(i) Relying on effective remedies against abuse once it has occurred ("curative mechanisms"), and

(ii) Providing means designed to prevent abusive registrations from occurring ("preventive mechanisms").

23. The most prominent example of a curative mechanism is the UDRP which was adopted by ICANN on the basis of recommendations made by WIPO in the First WIPO Report. Such curative mechanisms may in themselves also have a deterrent (and hence preventive) effect since they curtail the ability of abusive registrants to profit from their registrations and expose their practices.[11]

24. Many IP owners will, however, not consider curative remedies sufficient. In particular where the likelihood of abuse and the resulting damage is high, IP owners will require preventive protection. This presumption is corroborated by data showing that a significant number of domain names in the new gTLDs introduced as of November 2000 were registered for defensive purposes. Pursuant to the New gTLDs Report,[12] 41% of all domain names in these new gTLDs were registered for defensive purposes, 40% were not in use at all and 22% were used for a web site that merely redirected to another TLD; 80% of all registrants held domain name registrations in other gTLDs. The defensive registration strategy is however of limited use during the introductory phase of a new gTLD when IP owners will have to compete for their names on an equal footing with abusive registrants. Further safeguards offering preventive protection may therefore be necessary.

3.3 Types of gTLDs and Likelihood of Abuse

25. The likelihood of abuse and the corresponding need for preventive IP protection mechanisms will, in part, depend on the type of gTLDs that are introduced. The First WIPO Report suggested to draw a distinction between "open" TLDs, in which there are no restrictions on the persons or entities who may register in them, and "restricted" TLDs, in which only persons or entities satisfying certain criteria may register domain names.[13] The Report noted that:

"41. Where restrictions apply to the persons or entities that can register in a TLD, those restrictions may (but do not necessarily) provide means for reducing the tension between domain names and territorially based intellectual property rights. [...] for example, if the restriction applicable to the TLD defines carefully the type of entity that can register in the TLD, such as the requirement in .int that the registrant be an

---

11 The efficiency of the UDRP in preventing cybersquatting in existing and newly introduced gTLDs is explored in more detail below at paragraphs 36-52.

12 New gTLDs Report, page 100, *http://icann.org/tlds/new-gtld-eval-31aug04.pdf.* See also OECD Report at page 28.

13 First WIPO Report, paragraph 38.

international organization, this restriction may operate to reduce the potential for conflict between domain names and intellectual property rights, since it removes the possibility for commercial entities to register in the domain. We do not recommend that restrictions be introduced in respect of TLDs, but merely draw attention to the fact that restrictions can have an effect on the relationship between domain names and intellectual property rights.

"42. Where there are no restrictions that apply on registrations in a TLD, the potential for conflict between domain names and intellectual property rights is heightened."

26. The experience with the first round of new gTLDs also suggests that abuse is less likely in sponsored or restricted gTLDs -- at least if the registration restrictions are clear and either verified *ex ante* or enforceable *ex pos.*[14]. The likelihood of abusive domain name registrations will have a bearing on the type of IP protection needed. The more likely they are, the more rights owners will see a need for preventive measures. Otherwise, curative remedies may be sufficient.

4. New gTLDs in the First WIPO Internet Domain Name Process

27. The terms of reference of the First WIPO Internet Domain Name Process already included the IP aspects of new gTLDs. In this regard, the First WIPO Report recommended that:

"343. [...] on condition that the proposed improved practices for domain name registrations, the proposed administrative dispute-resolution procedure and the proposed measures for the protection of famous and well-known marks and for the suppression of abusive registrations of domain names are all adopted, new gTLDs can be introduced, provided that they are introduced in a slow and controlled manner which takes account of the efficacy of the proposed new practices and procedures in reducing existing problems."

28. The recommendation to establish exclusion mechanism for well-known marks was specifically made for new gTLDs[15] in order to meet the concerns of IP owners who

"249. [...] viewed exclusions as an indispensable safeguard in relation to the expansion of the DNS through the addition of new gTLDs. They feared the repetition of the experience of the last five years, in which the owners of famous and well-known marks have had to invest large amounts of human and financial resources in defending their marks against abusive domain name registrations."

---

14 See below, paragraphs 108-112.

15 First WIPO Report, paragraph 276.

29. The First WIPO Report also noted that

> "263 [...] it could be highly economically wasteful, in view of the experience in the existing open gTLDs over the past five years, to add new open gTLDs without any safeguard against the grabbing or the squatting of famous and well-known marks by unauthorized parties in those new open gTLDs."

30. The First WIPO Report proposed to limit the exclusion mechanism to famous and well-known marks for the following reasons:

- because famous and well-known marks are most likely to be a target of abusive practices in the DNS;[16]
- to give expression to the special protection for famous and well-known marks, over and above that accorded to other "ordinary" marks, in Article 6*bis* of the Paris Convention for the Protection of Industrial Property ("Paris Convention") and Article 16.2 and 16.3 of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement");[17]
- in response to concerns that exclusion mechanisms might lead to an erosion of the DNS through the removal of large numbers of names from its ambit.[18]

31. Under this mechanism,[19] owners of well-known marks could obtain an exclusion for their marks in all or some new open gTLDs. The exclusion would, however, not be granted automatically upon application, but pursuant to a decision by a panel of independent trademark experts, who would be appointed by an institution to review individual applications. The decision would have to be based on criteria developed on the basis of the international framework for the protection of well-known marks.[20] In the interest of efficiency and consistency, it was recommended to operate the mechanism centrally by a single provider competent in international IP issues, such as WIPO. Once granted, an exclusion would, in principle, be valid indefinitely. However, a third party with a legitimate interest in registering a domain name that is blocked by an exclusion could at a later stage

---

16 First WIPO Report, paragraph 246: "Famous and well-known marks have been the special target of predatory and parasitical practices on the Internet. The consultations held throughout the WIPO Process and the submissions made in them have confirmed the singular nature of these predatory and parasitical practices with respect to famous and well-known marks."

17 The protection of trademarks is, in principle, subject to the principles of territoriality and specialty, i.e. it is limited to specific territories as well as to specific goods or services. Well-known marks may enjoy protection that is wider both in terms of the territory as well as the goods and services covered. See the comprehensive legal analysis in paragraphs 252 to 262 of the First WIPO Report.

18 See First WIPO Report, paragraphs 250, 264 to 274.

19 The exclusion mechanism is described in more detail in paragraphs 276 to 291 of the First WIPO Report; Draft Rules for Panel Procedures Concerning Domain Name Exclusions are provided in Annex VII of the First WIPO Report.

20 The suggested criteria are set out in paragraphs 283 to 287 of the First WIPO Report.

apply to have the exclusion cancelled in respect of any of the gTLDs for which it was granted. The cancellation would then enable the third party to register the disputed domain name.

32. Since the exclusion would be granted only in respect of a string that is identical to the famous mark, it would not prevent close phonetic or spelling variations of the well-known mark from being registered as domain names in bad faith. To combat such abuse, the trademark owner could only rely on curative relief provided under the UDRP (or national court systems). To facilitate this, the First WIPO Report recommended:

> "291. [...] that the granting of an exclusion give rise to an evidentiary presumption, in favor of the holder of an exclusion, in the administrative procedure in such a way that, upon showing that the respondent held a domain name that was the same as, or misleadingly similar to, the mark that was the subject of an exclusion and that the use of the domain name was likely to damage the interests of the holder of the exclusion, the respondent would have the burden of justifying the registration of the domain name."

33. While the proposed exclusion mechanism was not implemented in practice, it is in some respects similar to the defensive registrations later offered by .name further described below.[21] Like a defensive registration, an exclusion would not resolve to an active domain name, but would primarily serve to remove a certain string from the pool of generally available domain names. This reflects the apparent interests of trademark owners, who have proven to be more concerned about defending their marks in new gTLDs than interested in getting additional domain name registrations. However, unlike defensive registrations which are limited to .name, an exclusion would provide protection across all open gTLDs and be granted only upon prior verification by independent panels. In terms of timing, the exclusion mechanism would have to be made available to trademark owners before the general registration ("Sunrise"), and could continue to be available later with regard to names that were not registered as domain names.

5. New gTLDs in the Second WIPO Internet Domain Name Process

34. The Second WIPO Internet Domain Name Process did not provide additional recommendations regarding the introduction of new gTLDs but, with regard to the first round of new gTLDs, made the following observation:

> "35. It is too early in the process of the introduction of the new gTLDs to assess what impact, if any, they will have on intellectual property. The introduction of the new gTLDs will be closely monitored by all and, in particular, from the perspective of intellectual property, with respect to the following issues:

---

[21] See paragraphs 95-103 below.

(i) the effectiveness of sunrise and other procedures for reducing the bad faith violation of trademark rights during the start-up phase of new gTLDs;

(ii) the impact of increased differentiation in the DNS upon the interface between domain names and intellectual property rights and whether increased segmentation in the DNS will create greater space for brand differentiation or increase the number of problems experienced with respect to the bad faith violation of intellectual property rights through domain name registrations;

(iii) the response to greater differentiation in the DNS on the part of Internet users, search engines and directory services; and

(iv) the design and inter-relationship between WHOIS services across an extended DNS."

35. These issues can now be reviewed in light of the experience made with the first round of new gTLDs.

6. The WIPO UDRP Experience

6.1 Background

36. The experience gained under the UDRP can provide information on its efficiency in providing curative relief, and on its preventive effect in discouraging cybersquatting. It can also be helpful in assessing the impact (if any) of the first introduction of new gTLDs on cybersquatting and enforcement patterns.

37. As stated earlier, the First WIPO Report recommended, among other measures, the establishment of a mandatory administrative dispute resolution procedure uniform across open gTLDs.[22] Following these recommendations, ICANN adopted the UDRP on August 26, 1999. The UDRP applies to every domain name registered in the following gTLDs: .aero, .biz, .com, .coop, .info, .museum, .name, .net, .org, and .pro by virtue of a dispute clause in the domain name registration contract. A UDRP decision ordering transfer or cancellation of the domain name is directly implemented by the relevant registrar. ICANN has accredited a number of institutions to provide dispute resolution services under the UDRP,[23] with the WIPO Center processing between 50-60% of all UDRP cases. The UDRP case information included in this section will, unless otherwise stated, be based on UDRP

---

22 First WIPO Report, paragraphs 129 to 244; a draft "Policy on Dispute Resolution for Abusive Domain Name Registrations" and related Rules are provided in Annexes IV and V of the First WIPO Report.

23 For a list of all ICANN-accredited UDRP dispute resolution service providers, see *http://www.icann.org/dndr/udrp/approved-providers.htm*.

cases involving gTLD domain names[24] administered by the WIPO Center since December 1999 through 2004.[25]

38. The UDRP procedure is time- and cost- effective, in particular considering the international context of the disputes. A domain name case filed with the WIPO Center is normally concluded within two months, and the applicable fee in most cases is 1,500 United States dollars.[26] Due process and transparency are ensured. The WIPO Center assists parties in filing their submissions by having created a model complaint, a model response and detailed filing guidelines. The Center has also developed a searchable online Index of WIPO UDRP Panel Decisions as well as a more concise overview of trends in WIPO UDRP panel decisions, which facilitate access to the thousands of WIPO decisions rendered thus far and enhance the predictability and consistency of decision-making under the UDRP.[27]

6.2 WIPO UDRP Case Filing

39. A first indicator of the general acceptance of the UDRP by the trademark community is the amount of cases filed under the Policy, despite the possibility of bringing the dispute before a national court. From the first UDRP case in December 1999 through the end of 2004, 6,692 cases have been filed with the WIPO Center; in 2,968 cases (44%) both parties were from the same country, a situation in which court litigation would have been a viable option. The filing rate has been at its highest in the first two years following the adoption of the UDRP (years 2000 and 2001), and has since gradually stabilized at 3.0 cases per calendar day until 2004, when the WIPO Center witnessed a 5.4% increase of cases compared with the previous year.

	2000	**2001**	**2002**	**2003**	**2004**
WIPO Filing Rate per calendar day	5.0	4.1	3.2	2.9	3.0

---

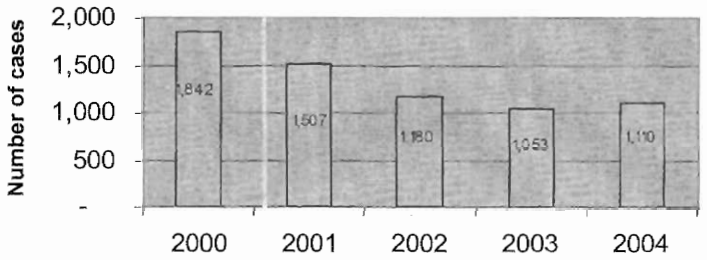
24 The WIPO Center also provides domain name dispute resolution services to certain ccTLDs, a number of which have adopted the UDRP on a voluntary basis. See the WIPO Center's web site at *http://arbiter.wipo.int/domains/cctld*. Unless otherwise indicated, the statistical information included in this Report does not cover ccTLD cases administered by the WIPO Center.

25 Unless otherwise indicated, the single UDRP case filed in December 1999 and decided in 2000 is included in 2000 figures.

26 The WIPO Center's Schedule of Fees is available at *http://arbiter.wipo.int/domains/fees*.

27 The WIPO Center's model forms, filing guidelines,online index of decisions and overview of decision trends are available at *http://arbiter.wipo.int/domains*.

WIPO UDRP Case Filing Rate



	2000		2001		2002		2003		2004		AVERAGE	
1	1,399	75.9%	1,153	76.6%	944	79.9%	833	79.1%	880	79.3%	1,042	77.8%
2	242	13.2%	164	10.9%	128	10.8%	128	12.2%	111	10.0%	155	11.6%
3 or more	201	10.9%	189	12.6%	109	9.2%	92	8.7%	119	10.7%	142	10.6%

40. The stabilization of the filing rate may in part result from more selective enforcement policies of trademark owners, which would reflect developments in the ".com economy" more generally. Moreover, the large number of cases filed during the first two years of the UDRP is in large part due to the backlog of disputes that had remained unresolved for lack of an inexpensive and efficient resolution system, until the adoption of the UDRP. Since then, the UDRP is increasingly used to resolve disputes resulting from subsequent domain name registrations. This conclusion is reinforced by an analysis of the last one hundred domain names disputed in cases filed with the WIPO Center in 2004. An overwhelming majority of these domain names have been registered subsequent to the adoption of the UDRP; 60 % were registered in the preceding two years.

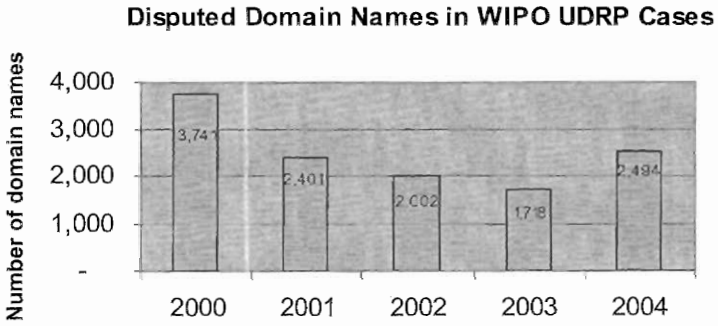
Sample of 100 disputed domain names before the WIPO Center in December 2004

Domain Name Registration Date	**Up to 1999**	**2000**	**2001**	**2002**	**2003**	**2004**
Percentage of Disputed Domain Names	8.1 %	5.4 %	11.7 %	15.3 %	19.8 %	39.6 %

41. Since a single UDRP complaint may relate to more than one domain name (if the multiple domain names are held by one person/entity), the number of disputed domain names outnumbers the number of actual cases. Through the end of 2004, the 6,692 cases filed

before the WIPO Center involved 12,355 domain names.[28] The WIPO average is 1.8 disputed domain names per case. In 78.5% of WIPO cases, the complaint relates to one domain name, in 11.6%, two domain names, and in 10.6% of cases there are three or more disputed domain names. These figures have remained fairly stable over the years.

42. The following graph shows the number of gTLD domain names disputed before the WIPO Center from 2000 through 2004, which generally follows the number of cases filed. Due to a number of cases involving particularly large numbers of domain names in 2004,[29] the increase in the number of disputed domain names in 2004 is slightly sharper than the increase in the number of cases in the same year.



43. The above data on the number of domain names per case do not indicate a significant concentration of cases among fewer parties, which might have been a sign of shifts in enforcement or cybersquatting patterns. This finding is confirmed by data on the number of different complainants and respondents involved in UDRP cases. The following table shows that this number has also remained fairly stable over the years.[30] The slight reduction in the percentage of respondents in 2003 and 2004 could indicate the beginning of a trend towards a concentration of cases among fewer but more active cybersquatters, but it is still too early to draw definitive conclusions.

---

28 A full list of disputed domain names is available in the table of cases on the WIPO Center's web site at *http://arbiter.wipo.int/domains/cases/all.html.*

29 In particular WIPO Case No. D2004-0821 involving 277 domain names and WIPO Case No. 2004-0400 involving 108 domain names.

30 The number of complainants and respondents has been counted on the basis of names provided in complaints and/or responses. For example, if a single domain name registrant uses multiple aliases and is named under such different aliases in different cases, it will be counted as multiple respondents. As a result, the actual numbers may be lower.

	Number of Cases	Number of Complainants		Number of Respondents	
2000	1842	1422	77%	1865	101%
2001	1507	1253	83%	1541	102%
2002	1180	1012	86%	1165	99%
2003	1053	872	83%	970	92%
2004	1110	906	82%	1036	93%

6.3 TLD Distribution in WIPO UDRP Cases

44. The distribution of gTLDs in UDRP cases may be taken as an indicator of the cybersquatting, and related enforcement, activity directed at individual domains. When the total number of 12,355 domain names involved in WIPO UDRP cases is broken down by gTLD, it becomes apparent that .com domain names are by far predominant.

	2000		2001		2002		2003		2004	
.BIZ	-	*0.0%*	2	*0.1%*	74	*3.7%*	33	*1.9%*	90	*3.6%*
.COM	2,696	*72.1%*	1,864	*77.6%*	1,456	*72.7%*	1,376	*80.1%*	2,101	*84.3%*
.INFO	-	*0.0%*	16	*0.7%*	115	*5.7%*	50	*2.9%*	58	*2.3%*
.NET	649	*17.4%*	334	*13.9%*	234	*11.7%*	175	*10.2%*	156	*6.3%*
.ORG	394	*10.5%*	185	*7.7%*	123	*6.1%*	84	*4.9%*	87	*3.5%*

45. Notwithstanding the addition of new gTLDs, the dispute ratio of .com domain names has increased by more than 10% between 2000 and 2004. The number of disputed .net and .org domains has declined by more than half in the same period. Dispute rates concerning domain names registered in the new .biz and .info domains are fluctuating. In 2002, the .biz domain contributed 3.7% of all domain names involved in WIPO UDRP disputes; this figure dropped to 1.9% in 2003 but then rose back to 3.6% in 2004. Disputes in the .info domain were at their highest in 2002, following their introduction in 2001, but have gradually declined since. The relatively high number of disputes in 2002 involving .biz and .info domain names may be explained by trademark owners' specific efforts in combating bad faith registrations in these new gTLDs once they had been made available. It should be noted, however, that these numbers were never even close to those of .com.

46. Comparing the number of disputed domain names per gTLD with worldwide registrations yields what may be referred to as the "cybersquatting ratio" of individual gTLDs. The following table shows data provided for the worldwide domain name registrations in the .biz, .com, .info, .net, and .org gTLDs during 2000-2004.[31]

[31] Source: *http://www.zooknic.com/Domains/counts.html.*

	2000		2001		2002		2003		2004	
.biz	-	*0.0%*	-	*0.0%*	817,501	*2.7%*	942,946	*2.7%*	1,060,193	*2.4%*
.com	20,652,200	*76.5%*	23,198,677	*74.9%*	21,991,795	*73.5%*	25,849,965	*74.0%*	31,931,475	*72.3%*
.info	-	*0.0%*	647,111	*2.1%*	1,000,901	*3.3%*	1,082,099	*3.1%*	2,843,330	*6.4%*
.net	3,888,091	*14.4%*	4,320,416	*14.0%*	3,684,679	*12.3%*	4,293,719	*12.3%*	5,113,766	*11.6%*
.org	2,446,840	*9.1%*	2,796,403	*9.0%*	2,426,220	*8.1%*	2,750,696	*7.9%*	3,201,915	*7.3%*

47. If the proportion of the disputed domain names in each gTLD space is expressed as a share of the domain name registrations worldwide, the .com TLD remains by far the most contentious space. While the proportion of .com registrations has gone down from 76.5% to 72.3% percent over the last five years, the proportion of disputes in the .com space has actually increased from 72.1% to 84.0% over the same period. Accordingly, the cybersquatting ratio of the other gTLDs is far lower than that of .com. Hence, .com is the most attractive space not only for trademark owners but also for cybersquatters. Of course, as one of the oldest open gTLDs, it continues to be closely associated with commercial activity on the Internet, despite the availability of other gTLDs.[32]

48. Among the new gTLDs, disputes have concentrated in .biz and .info, the new open spaces. That the number of disputes in these two gTLDs is low compared to .com may result from their comparatively limited appeal to trademark owners and cybersquatters thus far. Arguably, it may also indicate that the start-up IP protection mechanisms developed by these gTLDs have had some effect in discouraging cybersquatting.[33] There has been only one UDRP dispute in each of .aero and .name and none in .coop, .museum, and .pro. Hence, cybersquatting activities in the latter domains appear to be curtailed by the restricted nature of these domains.

6.4 WIPO UDRP Case Outcome

49. An analysis of the outcome of UDRP cases can indicate the level of cybersquatting activity in individual gTLDs: a higher (or lower) success rate of complainants in a given gTLD may indicate a higher (or lower) level of cybersquatting activity in that gTLD. In total, the rate of transfer decisions rendered WIPO panels has increased slightly over the last five years from 81% to 86%, probably as a result of increased predictability of UDRP decisions, which enables trademark owners to file mostly cases which have a reasonable chance of

---

[32] See also New gTLDs Report page 109: "notwithstanding greater choice, .com remains the TLD of first choice for a majority of gTLD registrants, including new registrants. Indeed, the decision whether to select a new gTLD is often dictated by the availability of .com. In nearly every interview, registrants, users and registries acknowledged a preference for the .com version of a registration if it is available."

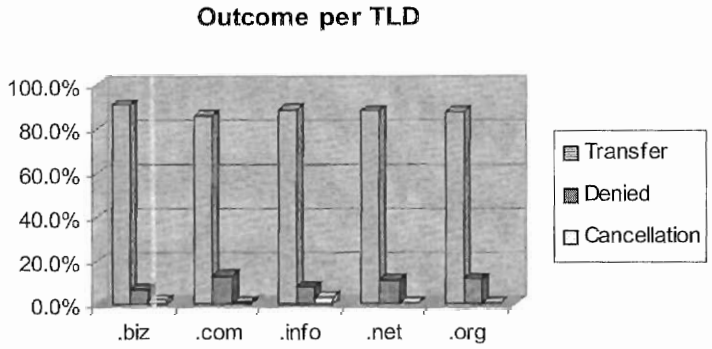
[33] These mechanisms are analyzed in more detail in paragraphs 57 to 103 below. The increase of disputes in the .biz domain in 2004 may be the result of a growing interest both by trademark owners and cybersquatters in this domain for its growing commercial recognition.

success. The table below shows the outcomes of WIPO UDRP decisions per year[34].

	2000		2001		2002		2003		2004	
Transferred	1,169	80.6%	963	78.7%	785	82.5%	732	86.4%	727	86.3%
Complaint Denied	275	18.9%	249	20.4%	155	16.3%	107	12.6%	106	12.6%
Cancellation	7	0.5%	11	0.9%	11	1.2%	8	1.0%	9	1.1%

50. The outcome is largely consistent across TLDs. While the comparatively low absolute numbers of cases in .info and .biz make it difficult to attach statistical significance to such figures, complainants were on average more likely to prevail in disputes involving .biz and (to a lesser extent) .info domain names in the first months following their introduction; probably because a larger number of famous names were still available for cybersquatting in these new gTLDs, which, in turn, resulted in a larger percentage of clear cases of cybersquatting.

	.biz			.info			Overall gTLDs		
	Transfer	**Denied**	**Cancelled**	**Transfer**	**Denied**	**Cancelled**	**Transfer**	**Denied**	**Cancelled**
2001	-	-	-	75.0%	25.0%	0.0%	85.6%	13.6%	0.8%
2002	93.9%	6.1%	0.0%	88.3%	9.6%	2.1%	85.1%	14.1%	0.8%
2003	92.2%	7.8%	0.0%	87.2%	11.3%	1.5%	85.5%	13.6%	0.9%
2004	93.4%	4.8%	1.8%	86.6%	10.4%	3.0%	86.7%	12.5%	0.8%



6.5 Evaluation

51. The UDRP has gained a considerable reputation for effective and predictable curative relief and, to some extent, for its preventive effect. Still, the above statistics show that the UDRP cannot fully eliminate cybersquatting. Cybersquatting continues despite the proven efficiency of the UDRP in providing curative relief, the media attention that the UDRP has been receiving, and the fact that thousands of domain name registrants have had their

[34] This table does not include those cases which were terminated for other reasons, in most cases because of a settlement reached between the parties.

registrations transferred to trademark owners. Abusive registration and use of domain names can still be attractive since the cost of registering a domain name has decreased over the last years, while some trademark owners may be prepared to pay to a domain name holder up to the amount they would have to spend in a UDRP procedure in exchange for the transfer of the disputed domain name. In addition, a domain name holder may be able to profit from misdirected Internet traffic (e.g. by virtue of advertisements placed on its web site) during the time it takes for the trademark owner to take effective action. Cybersquatting continues and, notwithstanding the availability of the UDRP, will likely also affect new gTLDs.

52. The introduction of new gTLDs does not seem to have caused significant changes in cybersquatting or enforcement patterns. The introduction of new gTLDs has not substantially increased the total number of cases, nor caused significant shifts in the distribution of affected gTLDs. UDRP disputes continue to concentrate heavily in the .com domain, and this trend has become even more manifest after the first round of new gTLDs was introduced. While this may partly be explained by the availability of the start-up IP protection mechanisms adopted by .biz and .info, it more likely indicates that, like trademark owners, cybersquatters are showing comparatively little interest in these new domains.[35]

7. The WIPO New gTLD Experience

53. The experience gained in the context of the first expansion of the DNS, which started in November 2000 with the selection of seven new gTLDs, provides valuable insight in related IP issues. ICANN regarded this first step towards more gTLDs as a "proof-of-concept" designed to test different ways of introducing new gTLDs. ICANN therefore adopted an experimental approach, selecting different types of gTLDs with different features.

54. Some of these new gTLDs are restricted to specific purposes. Thus, .aero is only available to the air transport community, .coop to cooperatives, .museum to museums, and .pro to qualified professionals; .biz is intended for *bona fide* business purposes and .name for personal names; only .info does not provide for any restrictions. Three of the restricted gTLDs, .aero, .coop and .museum, are "sponsored" gTLDs, whereas .biz, .info, and .pro are "unsponsored." In ICANN terminology,

> "an unsponsored gTLD operates under policies established by the global Internet community directly through the ICANN process, while a sponsored gTLD (i.e., .aero, .coop, and .museum) is a gTLD that has a sponsor representing a narrower community that benefits from the gTLD. The sponsor thus carries out delegated policy-formulation responsibilities over many matters concerning the sponsored gTLD."[36]

---

35 See the figures provided by the New gTLDs Report at page 99 which show that, at the end of 2003, actual registrations in .info and .biz constituted only 39% and 61% of the projections made by these registries before their launch.

36 See for example ICANN, Strategy: Introduction of New Generic Top-Level Domains, 30 September 2004, page 7, posted at *http://www.icann.org/tlds/new-gtld-strategy.pdf.*

55. As far as the protection of IP rights is concerned, a basic and ongoing level of protection is guaranteed by the UDRP which applies to domain names registered in all new gTLDs. In addition, there are two further types of dispute resolution policies. First, restricted and sponsored gTLDs provide a dispute resolution mechanism for violations of the registration conditions that are particular to that domain (e.g., the Restrictions Dispute Resolution Policy for .biz, which domain is restricted to "*bona fide* business or commercial purposes" or the Charter Eligibility Dispute Resolution Policy for the sponsored gTLDs). Second, some registry operators of the new gTLDs have introduced specific mechanisms designed to provide trademark owners with additional options for the protection of their rights during the introductory phase of these domains.

56. With regard to the second type of policies, under ICANN's experimental approach several different such trademark protection mechanisms were introduced at almost the same time, often under considerable time pressure. This led to considerable confusion among actual and potential registrants, registrars, and the broader community during the launch of the new gTLDs.[37] While introductory IP protection mechanisms were developed by the gTLD operators themselves, the WIPO Arbitration and Mediation Center was involved in their implementation for the purpose of administered resulting disputes. This involvement provided an insight in the relative strengths and weaknesses of the mechanisms concerned. On two of these mechanisms, the Afilias Sunrise Registration Challenge Policy for .info[38] and the Start-Up Trademark Opposition Policy for .biz (STOP),[39] the WIPO Center has published extensive reports which form the basis for the following two chapters.

7.1 .INFO: Sunrise Registration and Sunrise Challenges

57. Afilias, the registry operator of .info, provided trademark owners an option to register domain names before the general public during a "Sunrise Registration Period" which lasted from July 25 to August 27, 2001. Pursuant to the Sunrise Registration Conditions ("Conditions"), such Sunrise domain names had to be identical to the textual elements of a current trademark registration of national effect that was issued prior to October 2, 2000. Pursuant to the New gTLDs Report, Afilias received 80,951 Sunrise applications which resulted in 51,764 domain names.[40]

58. A crucial deficiency of the Sunrise system as implemented by .info was that compliance with the Conditions was not verified, even on a perfunctory *prima facie* basis, before registration. This tempted a great number of parties without trademark rights to abuse a

---

37 Similar conclusion in New gTLDs Report, page 22.

38 WIPO End Report on Case Administration under the Afilias Sunrise Registration Challenge Policy for .info, *http://arbiter.wipo.int/domains/reports/info-sunrise/index.html.*

39 WIPO End Report on Case Administration under the Start-Up Trademark Opposition Policy for .biz, *http://arbiter.wipo.int/domains/reports/biz-stop/index.html.*

40 New gTLDs Report, page 18.

registration option that had been created to protect genuine trademark owners. Instead of verifying Sunrise applications, Afilias offered a "Sunrise Challenge Period" (for the general public from August 28 to December 26, 2001; for the Registry after December 26, 2001) during which third parties could challenge Sunrise registrations for non-compliance with the Conditions. Such challenges were subject to the Afilias Sunrise Registration Challenge Policy for .info (the "Policy") and administered exclusively by the WIPO Center.

59. The Policy worked as follows: during the Sunrise Challenge Period anyone could file a challenge against a Sunrise registration alleging that it did not comply with the Conditions. If a Sunrise registration was challenged more than once, all challenges were queued in accordance with the date and time they were received by the WIPO Center. While, in practice, most disputed domain names did not have queued challenges, some of the most sought-after domain names involving generic words, such as <business.info> (6 challenges) or <realestate.info> (7 challenges), had multiple challenges. Priority Challengers, who ranked first in the queue, were invited to file a challenge and required to pay a challenger's fee of 295 United States dollars, consisting of a non-refundable part of 75 United States dollars, and a refundable part of 220 United States dollars (refunded when the challenger prevailed provided that the respondent had paid the respondent's fee).

60. If challenged by a third party, Sunrise registrants had 10 days to pay the respondent's fee of 295 United States dollars and 60 days to provide a trademark certificate showing that their registration was in compliance with the Conditions. If the respondent defaulted, the challenge was granted without further examination. If the respondent established its compliance with the Conditions, the challenge was dismissed and respondent's fee was refunded in full.

61. Unlike procedures under other domain name dispute resolution policies administered by the WIPO Center, Sunrise challenges were decided by the WIPO Center itself, i.e., without the appointment of external panelists. The WIPO Center's decisions were based solely on a *prima facie* examination of any trademark or service mark certificate submitted by a respondent and/or, following a revision of the applicable policy as explained below, by a challenger seeking transfer of the domain name. In a limited number of cases, the WIPO Center, in accordance with the Rules for Afilias Sunrise Registration Challenge Policy for .info (Rules), consulted relevant national IP offices in the context of reaching its determination. In some cases the trademark certificates that had been submitted turned out to be forged.

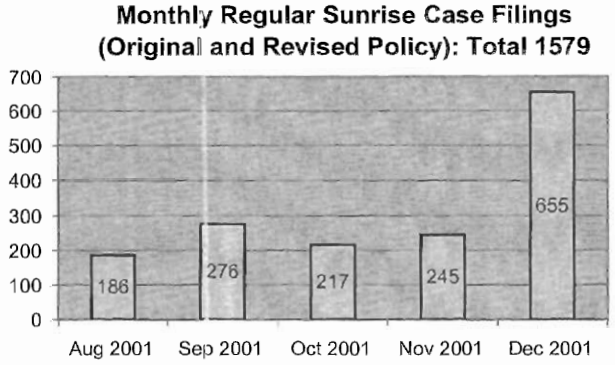
62. A problem of the Policy and Rules resulted from the fact that under its original version ("Original Policy," "Original Rules"), a challenger could successfully challenge a registrant and obtain a decision of transfer without itself having to prove compliance with the Conditions. While such transferred domain names could be the subject of new challenges, this was possible only during the Sunrise Challenge Period so that the last challenger was likely to retain the domain name. As a result, a substantial number of Sunrise challengers

without relevant trademark rights used the Sunrise Challenge mechanism to secure valuable names before they became available to the general public. In order to stop such abuse, the WIPO Center assisted Afilias in drafting a modified Policy and Rules which became effective on December 5, 2001 ("Revised Policy," "Revised Rules"). Under the Revised Policy, challengers requesting transfer were required to prove their compliance with the Conditions by submitting an original or a certified copy of a trademark certificate.

63. In order to clear the high amount of non-compliant Sunrise registrations, the Revised Policy and Rules also enabled Afilias to itself file challenges against registrations that appeared to have been made in violation of the Conditions, but that (e.g. because of their generic character) had remained unchallenged by third parties. These "Challenges of Last Resort" required the Registry to review all Sunrise domain name registrations. The Registry's serious efforts notwithstanding, its selection of names in respect of which it filed Challenges of Last Resort met with criticism. While a number of clearly fraudulent Sunrise registrations remained unchallenged, the Registry did challenge a number of good-faith trademark owners whose Sunrise registrations did not strictly meet the Conditions, because of slight differences between domain name and trademark or because the corresponding trademarks were only issued after October 2, 2000 (even though they had been applied for prior to that date).

7.1.1 Statistics

64. The WIPO Center received a total of 15,172 challenges. This caseload was comprised of 1,579 challenges filed by third parties during the Sunrise Challenge Period ("Regular Sunrise challenges") (equivalent to an average filing rate of 12.3 challenges per calendar day) and of 13,593 Challenges of Last Resort filed by the Registry between January 11, 2002 and April 8, 2002 (equivalent to an average filing rate of 154.5 challenges per calendar day).

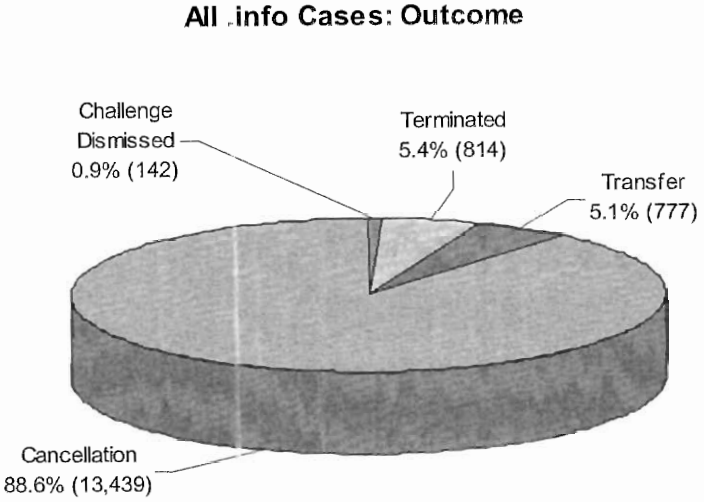


65. A significant proportion of the challenges involved domain names comprising generic words, e.g. <adoption.info>, <baseball.info>, <business.info>, <cars.info>,

<creditcards.info>, <football.info>, <golf.info>, <med.info>, <mobilephone.info>, <news.info>, <movie.info>, <sex.info>, <software.info>, <tech.info>, <travel.info>, <weather.info>, <wireless.info>.[41] Geographical terms, especially country names and city names, were also routinely challenged. With respect to the latter category, challenges filed by cities themselves were often unsuccessful under the Revised Policy for lack of registered trademark rights. Trademarks, such as those of well-known companies, were involved to a significantly lesser extent. This may be due to a variety of factors, in particular (i) the substantial amount of valuable generic terms that were registered in violation of the Conditions, (ii) the abuse of the Original Policy by non-trademark owners, and (iii) the lesser attractiveness of .info for trademark owners as compared to the .com domain.

66. The requirement under the Revised Policy for challengers seeking transfer to submit an original or a certified copy of a valid trademark certificate led to a decrease in the filing rate of challenges requesting transfer and an increase in the filing rate of challenges requesting cancellation.[42] Among the challenges filed under the Original Policy, an average of 5.5% of the challenges requested cancellation of the domain name registrations. Under the Revised Policy, that number increased to 21.2%.

67. Of all 15,172 Sunrise challenges, 14,216 (93.7%) were decided in favor of the challenger, and 142 (0.9%) were denied. 814 (5.4%) cases were terminated.



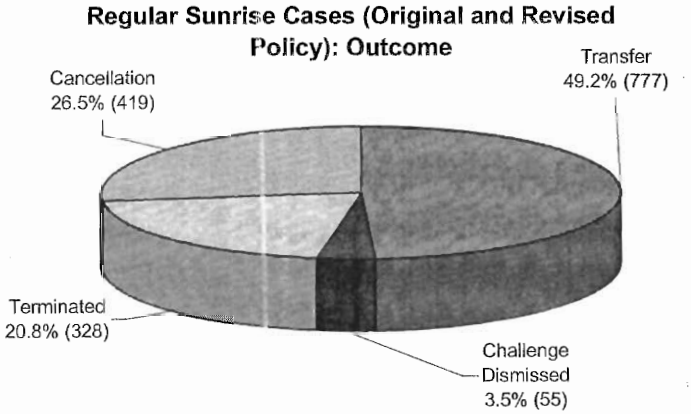
68. Of the 1,579 Regular Sunrise challenges, 1,196 (75.7%) were decided in favor of the Challenger, and 55 (3.5%) were denied. 328 (20.8%) cases were terminated primarily on the basis of payment deficiencies on the part of Challengers. These results break down as follows

---

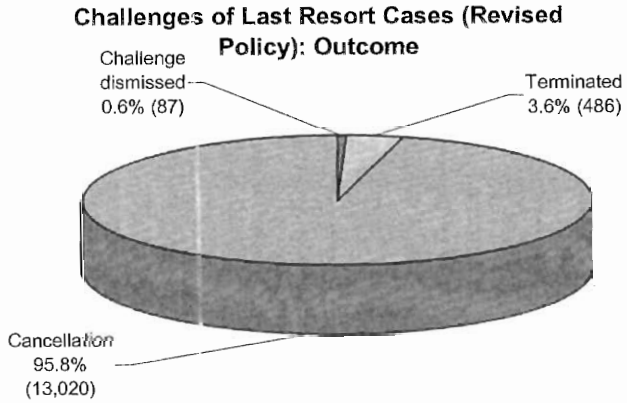
41 A list of all .info Sunrise challenges is available at *http://arbiter.wipo.int/domains/decisions/index-info.html.*

42 Challengers requesting cancellation were generally hoping to register the disputed domain once it became available for registration by the general public.

per Policy. Under the Original Policy, 719 (89.4%) decisions were rendered in favor of the Challenger, 651 (90.5%) of which were default judgments, i.e. findings in favor of the Challenger on the basis of the Respondent's default in the proceedings. Under the Revised Policy, 477 (61.5%) decisions were rendered in favor of the Challenger, 78 (16.4%) receiving a transfer decision, and 399 (83.6%) receiving a cancellation decision. As stated earlier, pursuant to the terms of the Revised Policy, the WIPO Center did not issue an automatic default judgment in cases of Respondent default, unlike under the Original Policy, but examined the Challenger's trademark rights when the requested remedy was transfer.



69. The remedy requested in Challenges of Last Resort was limited to cancellation of the domain name registration. Of the 13,593 Challenges of Last Resort, 13,020 (95.8%) were decided in favor of the Challenger, Afilias, and in 87 (0.6 %) cases, the challenge was denied. A further 486 (3.6%) cases were terminated primarily upon a request of withdrawal from Afilias. The high cancellation rate reflects Afilias' pre-selection of the names for which it submitted the challenges.



7.1.2 Evaluation

70. The lack of verification of Sunrise registrations was clearly the biggest flaw in the Sunrise mechanism. Out of a total of 51,764 domain names registered during the Sunrise period, some 15,000 were successfully challenged and a further 7,000 were cancelled by Afilias when their holders failed to respond to requests for trademark information sent by Afilias, meaning that a total of 22,000, or 43% of all Sunrise registrations, were registered without (sufficient) trademark rights.[43] This may in part be due to communication problems. Many registrars apparently did not properly inform registrants that Sunrise registrations were subject to certain Conditions. Numerous registrants, in fact, complained that their registrar's marketing in this regard had already been misleading and Afilias itself indicated that it had considerable communication difficulties with a number of its registrars.

71. The Sunrise challenge mechanism, which had been developed as a means to police compliance with the Conditions, offered little incentive for (compliant) third parties to challenge non-compliant Sunrise registrations unless they had a reasonable chance of obtaining the domain name. It was therefore not a suitable remedy against abusive registrations of generic or geographical names in violation of the Conditions because challengers would not have been able to obtain transfer of the disputed domain name for lack of own trademark rights. Another source of abuse resulted from the fact that the Original Policy allowed challengers to obtain a domain name without proving own trademark rights. Such challenges merely perpetuated the irregular status of non-compliant Sunrise registrations by keeping them away from the pool of generally available domain names.

72. As a result of these deficiencies, non-compliant registrants could, and did, use the Sunrise mechanism as a means to secure valuable domain names (which often consisted of generic terms) before the general public. In order to remedy the effect of such abuse, Afilias had to file a great number of Registry Challenges to have the trademark credentials of Sunrise registrants verified, a task that could have better been performed before registration.

73. Other problems were caused by lack of clarity in the Conditions themselves: the requirement that the domain name be "identical" to the textual or word elements of a trademark led to some uncertainty. An explanatory footnote to this requirement in the Policy stated that:

> "Identity will be deemed to exist also where there is a space between the textual or word elements of the mark (e.g., service mark) and a hyphen is used or the elements are combined in the Domain Name (e.g., service-mark.info or servicemark.info). In all other respects, the Domain Name must be identical to the textual or word elements of the mark."

---

43 Figures in the New gTLDs Report, page 19.

This did not cover elements which, like an ampersand ("&"), formed part of the textual elements of a trademark but could not be reproduced in the domain name. The WIPO Center adopted a strictly literal approach, but accepted transcriptions of signs that, for technical reasons, could not be part of a domain name. On the other hand, the condition constituted a fairly low threshold since it also enabled holders of marks, which consisted of generic terms but could be registered as trademarks because of distinctive ornamental or scriptural features, to secure domain names corresponding to the non-distinctive word elements of their marks (although these elements did not enjoy trademark protection as such). It would probably have been fairer to limit the Sunrise mechanism to word marks.

74. Another source of uncertainty was the condition that trademarks had to be "issued" prior to October 2, 2000. Afilias interpreted this term as requiring the actual registration to have occurred before that date. This conflicted with the fact that trademark protection in most countries is granted retroactively as of the "priority date" which is usually the date of application. Differences in terminology led to inconsistencies since some countries distinguish between the effective date of trademark registration and the priority date, whereas others do not make this distinction and indicate the priority date as the effective registration date. The .info Policy did not leave the WIPO Center any choice but to accept only the registration date as shown on the trademark certificate as the valid date of registration. It would have been preferable to accept the priority date, provided, of course, that the mark had been registered at the time of domain name registration.[44]

75. A number of procedural problems highlight the importance of preparing and maintaining adequate cooperation among all actors involved in such a mechanism. The WIPO Center's administration of Sunrise disputes was dependent, in part, on Afilias' execution of its obligations under the Policy and Rules, primarily the provision of accurate information on the domain name registrant and the timely follow-up in relation to decisions rendered under the Policy. As the administrator of a newly established gTLD, Afilias had to deal with a wide range of start-up operations, merely one of which was the implementation of its untested Sunrise dispute resolution mechanism. Possibly as a result, the WIPO Center was faced with a number of difficulties.

76. Important problems resulted from deficiencies in the .info Whois register. Maintaining accurate Whois data for a disputed domain name is vital for the administration of a dispute resolution procedure. In the Sunrise challenge procedure, there were numerous instances where the Whois information for the disputed domain name was not updated and remained inaccurate. For example, Whois information showed the name of the losing respondent months after the WIPO Center had notified a transfer decision in favor of the challenger. This not only frustrated the process for the winning challenger, but also prevented the WIPO Center from determining the ownership status of the domain name as was necessary in cases

---

[44] This is the approach suggested in the new sTLD application of .mobi, *http://www.icann.org/tlds/stld-apps-19mar04/mobi.htm*: "Registered trademark owners applying under 1a or 1b above will need to demonstrate that the registered right relied upon was applied for prior to 10 March 2004."

involving queued challenges. As a further example, the information provided in the .info Whois would sometimes differ from the information provided in the concerned registrar's Whois. Many parties also complained of incorrect data registration by the concerned registrars, resulting in incorrect Whois information. A further complication resulted from the Afilias' blanket lock on the Whois information of all Sunrise registrations. Afilias did not allow any modifications in the Whois information. As a result, when a registrar or a registrant had, often erroneously and in good faith, entered certain information, there was no recourse available to correct such data. This, in turn, placed the WIPO Center in a difficult position, as the WIPO Center's decision had to be based on the (sometimes obviously inaccurate) information provided in the Whois.

7.2 .BIZ: IP Claims and STOP

77. Unlike .info, .biz did not provide trademark owners a preferential registration option, but attributed all domain names on a randomized basis during its start-up phase which lasted from June 25 to September 21, 2001. In order to obtain the domain names corresponding to their trademarks, right holders had to submit a domain name application and participate in the randomized attribution of domain names. Instead of a preferential filing option, .biz offered trademark owners the possibility to purchase "IP Claims" which, in essence, provided an automated "watch service" combined with a (potential) priority in enforcing their rights against abusive registrants in an administrative procedure under the "Start-up Trademark Opposition Policy" (STOP).

78. The IP Claim system worked as follows: between May 21 and August 6, 2001, trademark owners could, against a fee, register IP Claims in order to claim trademark rights in relation to an alphanumeric string that was identical to their trademark. Compliance with this condition was neither verified by registry operator NeuLevel nor by any registrar. Moreover, because the number of IP Claims that could be filed for a given alphanumeric string was not limited, every domain name could be subject to multiple IP Claims. Such multiple claims could be filed by different claimants, or even by one and the same claimant. It is reported that NeuLevel received a total of 80,008 IP Claims.[45]

79. If, during the start-up phase, an application was filed for a domain name that was subject to an IP Claim, NeuLevel first contacted the domain name applicant, provided details of all IP Claims filed for this domain name (including contact details of the IP claimants, as well as the trademark data provided) and requested the applicant to confirm its intention to register the domain name. According to the New gTLDs Report, applicants abandoned their application in 198,085 cases and proceeded to registration in 61,629 cases.[46] Any domain name that was subject to at least one IP Claim did not resolve (i.e. could not be used) for a period of 30 days after the live date of .biz start-up domain names. Following the 30-day

---

45 New gTLDs Report, page 37.

46 New gTLDs Report, page 37.

period, the domain name resolved but could not be transferred until all pending IP Claims were dealt with as described below.

80. If a domain name applicant proceeded to register the domain name in spite of the IP Claim, NeuLevel notified the concerned IP claimant of the contact details of the domain name registrant. If more than one IP Claim had been filed with regard to the disputed domain name, NeuLevel established a priority order among these claims on a randomized basis (STOP, paragraph 4(l)(i)). The priority claimant received a "ticket number" which identified it as priority claimant and was given 20 days to initiate a STOP proceeding. If the priority claimant failed to file its complaint during that period, NeuLevel notified the next claimant in the priority order of its right to file a STOP complaint.

81. STOP provided curative relief only against abusive registrations. In order to prevail, the complainant had to prove to a neutral panelist that

> (i) the disputed domain name is identical to a trademark or service mark in which the complainant has rights;
> (ii) the domain name registrant (respondent) has no rights or legitimate interests in respect of the domain name; and
> (iii) the respondent has registered or is using the domain name in bad faith.

If the complainant could prove these elements, the panelist issued a decision ordering transfer of the domain name and no further STOP complaints by any other IP claimants were accepted. If the complainant did not prevail, the complaint was dismissed and a subsequent IP Claimant was invited to file a STOP complaint, except where the respondent had demonstrated a right or a legitimate interest in the disputed domain name, in which case no further STOP complaints were accepted.[47]

82. STOP was closely modeled after the UDRP, with the following important differences:

- Under STOP, Complainants had to show identity (not merely confusing similarity) between the disputed domain name and their trademark or service mark, STOP, paragraph 4(a)(i);
- Under STOP, it was sufficient to prove either registration **or** — not "and" — use in bad faith, STOP, paragraph 4(a)(iii);
- The only available remedy under STOP was transfer and not also cancellation, STOP, paragraph 4(i);
- Parties could not opt for three-member Panels; STOP disputes were exclusively decided by single-member Panels, STOP, paragraph 4(e).

---

47 For the various types of decisions see STOP, paragraph 4(l)(ii) and STOP Rules, paragraph 15(e).

83. STOP took precedence over the UDRP (STOP, paragraph 5) so that, as long as a .biz domain name was, or could be, subject to a STOP proceeding, no UDRP complaint could be filed by others against that domain name.

7.2.1 Statistics

84. Out of a total of 801 STOP complaints,[48] 338 complaints covering 355 domain names were filed with the WIPO Center. 333 of these complaints concerned one domain name only; one complaint each referred to two, three, four, five and eight domain names, respectively. Considering the significant number of IP Claims sold, the number of STOP complaints actually filed proved very limited. This may have been due to the following factors:

- Since the IP Claim system was independent of the attribution of domain names, a considerable number of trademark owners who had filed both a domain name application and an IP Claim appear have to obtained the domain name in which they had claimed rights;

- In a considerable number of cases a single trademark owner had filed multiple IP Claims with regard to one and the same domain name;

- As stated above, many domain name applicants (who were not also the owner of the IP Claim) decided not to pursue their application when notified of the IP Claim;

- In several cases, the IP claimant may have realized that the domain name registrant was likely to have own rights in the disputed domain name and thus refrained from filing a STOP complaint;

- In the majority of cases where domain names were subject to multiple IP Claims, a STOP complaint initiated by the priority claimant led to a final determination so that no further challenges by other IP claimants were permitted.

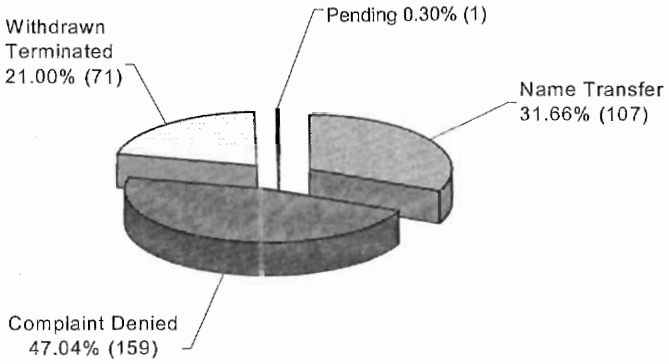
85. The overwhelming majority of WIPO STOP complaints were filed by priority claimants. Priority claimants challenged 295 (83%) of all .biz domain names subject to STOP proceedings administered by the WIPO Center. IP claimants with second priority initiated STOP complaints against 39 domain names (11%), 14 domain names (4%) were challenged by IP claimants with third priority, with smaller numbers for the lower priorities. Since transfer decisions were issued in 107 cases and 118 complaints were finally dismissed, in 225 out of 338 cases (66.57%), a STOP proceeding resulted in a final attribution of the domain name to either the complainant or the respondent, only in 41 cases (12.13%), the panel allowed further STOP complaints by subsequent IP claimants.

---

[48] Figure given in the New gTLDs Report, page 36.

86. The outcome of STOP proceedings administered by the WIPO Center differs from those of proceedings under the UDRP. Of the 338 STOP complaints, 107 (31.66%) were decided in favor of the Complainant, while 159 (47.04%) were denied and 71 (21.00%) cases were terminated. One case was suspended (0.30%) pending the outcome of a court action relating to the disputed domain name. In comparison, of the 990 UDRP complaints received within the same period (December 2001 to September 2002), 661 (66%) were decided in favor of the Complainant, 137 (14%) were denied, and 192 (20%) were withdrawn or terminated.

WIPO STOP Cases: Outcome



7.2.2 Case Results

87. The following STOP-specific factors may have contributed to the comparatively high rate of STOP complaint denials:

88. *High Amount of Generic, Descriptive or Suggestive Terms.*[49] A significant proportion of the 355 domain names challenged under STOP consisted of terms that can be considered as generic, descriptive or at least suggestive, such as <womenshealth.biz>, <menshealth.biz>, <games.biz>, <money.biz>, <dogracing.biz>, <bicycling.biz>, <scubadiving.biz>, <mountainbike.biz>, <postoffice.biz>, <management.biz>, <capital.biz>, <realestate.biz>, <4sale.biz>, or <guns.biz>. In such cases, panels typically were reluctant to find bad faith since there could be other plausible explanations for their registration than bad faith on the part of the respondent[50]. The significant share of generic domain names that were

---

49 Annex 3 of the STOP Report provides a list of all domain names challenged under STOP.

50 Cf. *Network Associates Technology, Inc. v. Lenow International, Inc.*, WIPO Case No. DBIZ2001-00043 <cybercop.biz>; *New York Stock Exchange, Inc. v. Manuela Lemmel*, WIPO Case No. DBIZ2001-00044 <e-broker.biz>; *The Boots Company Plc v. Challenge Services, Inc. (CSI)* WIPO Case No. DBIZ2002-00096 <boots.biz>; *Rodale, Inc. v. Kelly Britt*, WIPO Case No. DBIZ2002-00152 <bicycling.biz>; *Prisma Presse v. Orlik Software*, WIPO Case No. DBIZ2002-00177 <management.biz>; *Consignia Plc and Post Office Limited v. Aly Ramzan*, WIPO Case

subject to STOP proceedings may have resulted from the proven value of such terms in other TLDs on the one hand, and from confusion with the .info Sunrise scheme on the other which did not verify the trademark credentials of Sunrise registrants; as a result, some IP claimants seem to have believed that the mere fact that they had paid for the IP Claim and the STOP complaint would suffice to obtain the domain name.

89. *Difficulty of Proving Bad Faith in a Start-Up Situation.* The high number of dismissed STOP complaints also indicates that the three criteria listed in Paragraph 4(a) STOP were difficult to prove in a start-up scenario, even though STOP had lowered the threshold by only requiring proof of bad faith registration **or** use of the domain name. In practice, however, complainants could only attempt to prove bad faith registration since in almost all cases the disputed domain name had, for technical reasons, not been used at all.[51] The "Telstra" argument developed under the UDRP,[52] according to which passive holding of a domain name may in certain circumstances be considered as an indication of bad faith use, was advanced in some complaints but never accepted by panelists since the non-use of .biz start-up domain names resulted from technical restrictions rather than from a conscious decision of the registrant. Hence, complainants were *de facto* prevented from relying on any evidence of domain name use. Bad faith registration alone was, however, difficult to prove, in particular since the 20-days time limit left hardly any time for collecting convincing circumstantial evidence. In some cases, panelists took the fact that the respondent had proceeded to register the domain name in spite of having been notified of an IP Claim as an indication of bad faith.[53] Subsequent decisions clarified, however, that the notification was of little relevance where the disputed domain name was a generic or descriptive word, and where there was no evidence that the complainant's mark was well-known or at least known to the respondent.[54] As a result, complainants had a reasonable chance of prevailing under STOP only where their mark was both distinctive and well-known in the jurisdiction where the respondent was based since in such cases the domain name could only be understood as referring to the owner of the mark and no other legitimate uses could be imagined.[55]

No. DBIZ2002-00180 <postoffice.biz>; *Admiral Insurance Services Limited v. Diamond Trust Consultancy (UK) Limited*, WIPO Case No. DBIZ2002-00232 <diamond.biz>; *Mohawk Brands, Inc v. iSMER*, WIPO Case No. DBIZ2002-00242 <image.biz>; *Dan Zuckerman v. Vincent Peeris*, WIPO Case No. DBIZ2002-00245 <shoes.biz>; *AB Electrolux v. International Newcastle*, WIPO Case No. DBIZ2002-00260 <partner.biz>; *Zentralverband deutscher Konsumgenossenschaften e.V. v. eDesign Japan*, WIPO Case No.DBIZ2002-00261 <plaza.biz>; *target software solution GmbH v. NetVirtue, Inc.* WIPO Case No. DBIZ2002-00277 <target.biz>.

51 Priority Claimants had to file their STOP complaints within 20 days following the live date even though the domain names that were subject to an IP Claim did not resolve for 30 days.

52 see *Telstra Corporation Limited v. Nuclear Marshmallows*, WIPO Case No. D2000-0003.

53 *Rodale, Inc. v. Cass Foster*, WIPO Case No. DBIZ2002-00148, <menshealth.biz>.

54 *Mohawk Brands, Inc v. iSMER*, WIPO Case No. DBIZ2002-00242 <image.biz>; *Zentralverband deutscher Konsumgenossenschaften e.V. v. eDesign Japan*, WIPO Case No. DBIZ2002-00261 <plaza.biz>.

55 see e.g. *AUDI AG v. vitty Inc*, WIPO Case No. DBIZ2002-00027 <audi.biz>; *Fiat Auto. v. Italienska*, WIPO Case No. DBIZ2002-00030 <fiat.biz>; *Mastercard International Incorporated v. Mr. Greg Tieu*, WIPO Case No. DBIZ2002-00124 <mastercard.biz>.

90. *Lack of Identity between Trademark and Domain Name.* Unlike the UDRP, STOP required identity between the complainant's trademark and the disputed domain name. Generally, panelists considered it sufficient if the domain name was identical with the textual elements of the trademark that are technically reproducible in a domain name. Divergence in elements that cannot be included in a domain name, such as an ampersand sign or a space, was considered irrelevant.[56] If, however, certain elements of the trademarks were not included in the domain name even though that would have been technically feasible, panels refused to find identity.[57] A finding of identity was somewhat more problematic in cases involving device marks where the graphic or ornamental elements cannot be reproduced in a domain name. Some panelists were reluctant to find identity in such cases.[58] This would have had the effect of excluding such device marks from protection under STOP, which could be a conscious policy decision but should in this case be stated clearly. The question did, however, not have to be decided conclusively, since the complaints concerned were all dismissed on other grounds.

91. *Disputes Between Competing Right Owners.* Some complainants seem to have assumed that trademark ownership together with an IP Claim would suffice to prevail in a STOP proceeding. This may have been the reason why a number of complaints were brought against respondents who held own rights in the registered term.[59]

7.2.3 Evaluation

92. The .biz introductory trademark protection mechanism combined two elements: the IP Claim system and STOP. If trademark owners wished to obtain domain names corresponding to their rights, they were required to file separate domain name applications. Each element, i.e. the domain name application, the IP Claim and the STOP complaint, was subject to a separate fee. The resulting system was fairly costly and complex and, as outlined above,

---

56 e.g. *AT&T Corp. v. Swarthmore Associates LLC*, WIPO Case No. DBIZ2002-00077 <att.biz>; *Fiat Auto S.p.A v. Italienska bil*, WIPO Case No. DBIZ2001-00030 <alfaromeo.biz>.

57 e.g. *Hotel Lotte Co., Ltd. v Morris Communications Company, LLC*, WIPO Case No. DBIZ2002-00024 <charlotte.biz> as compared to the trademark THE CHARLOTTE SUITE; *H&M Systems Software, Inc. v. dotPartners LLC*, WIPO Case No. DBIZ2002-00063 <argos.biz> as compared to ARGOS GAMEWEAR; *Dan Zuckerman v. Vincent Peeris*, WIPO Case No. DBIZ2002-00245 <shoes.biz> as compared to SHOES.COM; *Asociación de Usuarios de Internet v. WorldWide Media Inc.*, WIPO Case No. DBIZ2002-00204 <internet.biz> as compared to INTERNET'99; *Osborne Clarke v. Blacker Media*, WIPO Case No. DBIZ2002-00262 <games.biz> as compared to GAMESBIZ.

58 *Qtech Business Systems Pty Ltd v. Coldwell Banker Burnet*, WIPO Case No. DBIZ2001-00004 <qtech.biz>; *The Boots Company Plc v. Challenge Services, Inc. (CSI)*, WIPO Case No. DBIZ2002-00096 <boots.biz>; *Souza Cruz S.A. v. Null*, WIPO Case No. DBIZ2002-00116 <personaltouch.biz>.

59 e.g. Actebis Holding GmbH v. peacock.com Corporation, WIPO Case No. DBIZ2001-00005 <peacock.biz>; Standard Knitting Ltd v. Toyota Motor Sales, USA, WIPO Case No. DBIZ2001-00011 <tundra.biz>; BUSS GmbH & Co. KG Fertiggerichte v. Steven Buss, WIPO Case No. DBIZ2001-00034 <buss.biz>; Brose Fahrzeugteile GmbH & Co KG v. Brose Systeme GmbH, WIPO Case No. DBIZ2002-00143 <brose.biz>; Ricardo Plc v. QXL Ricardo Plc, WIPO Case No. DBIZ2002-00240 <ricardo.biz>; Hay & Robertson International Licensing AG v. Admiral Insurance Services Ltd, WIPO Case No. DBIZ2002-00254 <admiral.biz>.

caused a good number of misconceptions. The fact that two completely different IP protection mechanisms were promoted by .info and .name at almost the same time certainly added to the confusion among registrants and registrars.

93. Unlike the .info Sunrise system, the .biz approach did not give trademark owners preference over other potential registrants. Instead, for the added expenses of participating in the IP Claim service, trademark owners were offered a watch service combined with a possibility (randomized in case of multiple IP Claims) to enforce their rights in a STOP proceeding against abusive registrants. Hence, .biz did not adopt a preventive approach to trademark protection, but instead offered trademark owners curative mechanisms that were modeled after the UDRP but slightly adapted to the start-up situation.

94. Since a high number of domain name applicants apparently did not proceed with their application after being notified of an IP Claim, the IP Claim system must have had a preventive effect. This in itself may be regarded as a success. For those trademark owners who had to proceed to a STOP complaint, however, the system was only of limited benefit since it proved truly effective only in protecting well-known trademarks against clear cases of cybersquatting – which may have been the result of a conscious policy decision. The protection provided did however not go beyond the UDRP which has proven to be an effective remedy against cybersquatting. In fact, since the UDRP is not limited to identical names but includes confusingly similar names, it offers a broader scope of trademark protection than STOP. It must be borne in mind, however, that the UDRP standard, which requires the complainant to prove bad faith in regard to both registration **and** use in bad faith, may limit its efficiency in a start-up context.[60]

7.3 .NAME: Defensive Registrations

95. The .name domain is an unsponsored gTLD that is restricted to registrations of personal names (described as the legal name of an individual or the name by which a person is commonly known) or names of fictional characters (provided the applicant holds a trademark or service mark right in that name). In .name, domain names and "SLD e-mail addresses" are both referred to as "Registered Names". Until recently, names could only be registered on the second and third level (e.g. <john.smith.name> or <smith.john.name> or <j.smith.name>). Following an amendment of the .name Registry Agreement with ICANN,[61] names can now also be registered directly at the second level (e.g. <smith.name>).

96. GNR, the operator of .name, offers trademark owners a "Name Watch Service" under which subscribers are alerted when a certain alphanumeric string ("Watched String") is registered. The same string may be on watch for different Name Watch registrants. Unlike

---

60 See below at paragraphs 114-115.

61 Amendment 1 of 8 August 2003 to the .name Registry Agreement, posted at *http://www.icann.org/tlds/agreements/name/registry-agmt-amendment-1-8aug03.htm*.

the IP Claim system developed by .biz, the Name Watch Service does not provide further benefits, such as a notification to domain name applicants or a preferential opportunity to initiate a dispute resolution procedure.[62]

97. In addition, trademark owners can purchase Defensive Registrations which cannot be used as active domain names but, depending on their type, block the registration of names containing the reserved string on either the second (second-level Defensive Registrations) or the third (third-level Defensive Registrations) or on both levels (combined second- and third-level Defensive Registrations). Since Defensive Registrations do not function as Internet addresses, the same Defensive Registration can be sold to different registrants. Despite the seeming simplicity of the concept, .name developed a highly complex system to implement it.

98. During "Phase I" which started with the general opening of .name during "Land Rush" and ended on June 13, 2002, Defensive Registrations were only available for trademarks (i) the textual elements of which were identical to the reserved string, that (ii) had national effect and (iii) were registered prior to April 16, 2001. Compliance with these conditions was not verified. Since the end of Phase I, there are no restrictions and anyone can register Defensive Registrations. Defensive Registrations are relatively costly and the number actually registered is limited: Pursuant to a recent report, 1,212 Defensive Registrations were registered between August 15 and December 14, 2001; the number later increased to 1,461.[63]

99. An applicant seeking to register a name that is covered by a Defensive Registration is notified accordingly. If the applicant nevertheless wishes to register the domain name, it can either seek consent from the holder of the Defensive Registration, or file a challenge against the Defensive Registration under the Eligibility Requirements Dispute Resolution Policy for .Name (ERDRP). Since a domain name application can be blocked by several overlapping Defensive Registrations, the holders of all these Registrations must either give their consent or be challenged under the ERDRP.

100. There is no up-front verification of compliance with the .name registration restrictions for Registered Names and Defensive Registrations. Instead, both can be challenged through an administrative dispute resolution procedure under the ERDRP on any or both of the following grounds:

- Applicant's own eligibility to register in accordance with registration restrictions for Registered Names (Paragraph 4(a)(iii) ERDRP);

---

62 Pursuant to the New gTLDs Report, page 52, there were only 257 NameWatch subscriptions between August 15 and December 14, 2001 and the number later fell to 132 subscriptions.

63 New gTLDs Report, page 52.

- Registrant's non-compliance with the registration restrictions for Defensive Registrations (if the Defensive Registration was registered in Phase I, paragraph 4(a)(ii) ERDRP);

101. If, in the latter case, the holder of the Defensive Registration is unable to prove its compliance with the relevant registration restrictions, the Defensive Registration is cancelled thus ceasing to block any conflicting Registered Name applications. In addition, a new procedure is initiated *ex officio*, in which the respondent is required to demonstrate its compliance with the eligibility requirements for any and all of its other Phase I Defensive Registrations (Paragraph 5(f)(iii) ERDRP).

102. If the applicant can prove its own eligibility to register the blocked Registered Name, it will be allowed to register the name in spite of the Defensive Registration. The fate of the challenged Defensive Registration depends on its type: if it is a combined second and third level Defensive Registration (and hence identical to the desired domain name), the Defensive Registration is cancelled (Paragraph 5(f)(ii)(B) ERDRP). Second or third level Defensive Registrations, which can continue to block other Registered Name applications, will be cancelled once they have been successfully challenged for the third time (Paragraph 5(f)(iii) ERDRP).

103. Until the end of 2004, the WIPO Center has administered only four cases under the ERDRP, all resulting from eligibility disputes involving Registered Names. There has as yet been no case involving a Defensive Registration. Moreover, the number of Defensive Registrations has remained small. Trademark owners may have considered cybersquatting in .name as less likely, or as less damaging, and therefore seen less of a need to engage in defensive or preemptive practices, in particular since the UDRP provides curative relief. The fact that there has been only one UDRP case involving a .name domain name supports the assumption that .name seems to be less attractive for cybersquatters. The expense and complexity of the system may also have deterred some trademark owners.

7.4 .PRO: Defensive Registrations

104. The .pro domain is an unsponsored gTLD registration in which is restricted to certain professionals, currently doctors, lawyers and accountants (.pro plans to extend its registration services to dentists, architects and engineers). Each registrant's identity and professional license information is verified against relevant public and third party databases prior to domain name activation. Typically, names are registered on the third level, with the second level indicating individual professions (<smith.law.pro>, <smith.cpa.pro>, <smith.med.pro>). Registrants who provide multiple professional services (e.g. legal and accounting services) are eligible to register a resolving second-level name (e.g. companyname.pro). In an initial phase, domain names can only be registered by professionals who are qualified to practice in certain jurisdictions, including Canada, Germany, the United Kingdom and the United States.

105. Like .name, .pro offers Defensive Registrations. Owners of valid registered trademarks can purchase an IP Defensive Registration which is identical to their mark. During the Sunrise Period (April 5 to May 14, 2004), this possibility was limited to trademarks registered prior to September 30, 2002. Depending on their type, IP Defensive Registrations block the registration of a certain alphanumeric string, as a domain name or (in this respect it differs from .name) a defensive registration, either across all profession-specific domains ("Premium Intellectual Property Defensive Registrations"), or in one such individual profession-specific domain only ("Basic Intellectual Property Defensive Registrations"). IP Defensive Registrations cannot be registered where conflicting domain name registrations have already been made. By the end of 2004, there was no publicly available information on the number of IP Defensive Registrations in .pro.

106. Any person can submit a challenge under the RegistryPro IP Defensive Registration Challenge Policy for .pro (IPDRP) arguing that a particular IP Defensive Registration is not in compliance with the IP Defensive Registration conditions. Unlike in .name, challenges cannot be based on the challenger's own eligibility to register a name. The challenger can request cancellation or transfer of the IP Defensive Registration. If so challenged, the holder will be required to prove its eligibility to register the IP Defensive Registration. Challengers requesting transfer of an IP Defensive Registration are required to submit trademark documents proving their own eligibility (Paragraph 3(a) IPDRP Rules). Challenges are decided by the WIPO Center on the basis of the trademark certificates provided by the parties without recourse to external panelists.

107. The WIPO Center is the only dispute resolution provider for IPDRP challenges. By the end of 2004, no such challenges were filed. This may be due to the late roll-out of .pro and its comparatively low total registration numbers which result from its highly restricted nature. In addition, the verification process may also have served to prevented abusive registrations. As a result, .pro is less likely to attract abusive domain name registrations and many trademark owners may perceive less of a need for defensive or preemptive measures, in particular since the UDRP continues to provide curative relief against cybersquatting. By the end of 2004, .pro domain names have not been the subject of any UDRP complaints filed with the WIPO Center.

7.5 Sponsored gTLDs: Eligibility Verification

108. As stated earlier, three of the seven gTLDs that were introduced as of November 2000, .aero, .coop, and .museum, are sponsored. The "sponsor" should represent a specific "community" and develop policies that apply to registrations in the sponsored gTLD. Registrations are generally limited to applicants coming from the community described in the gTLD's "charter". As a result, sponsored gTLDs tend to be less commercial and attract fewer domain name registrations than unsponsored gTLDs.

109. All sponsored gTLDs must verify compliance of applicants with the Charter before registration, admitting only applicants that form part of the group. As an additional safeguard against non-compliant registrations, the Charter Eligibility Dispute Resolution Policy (CEDRP) allows third parties to challenge domain names registered in violation of a sponsored gTLD's Charter. However, by the end of 2004, no such CEDRP challenges have been filed with the WIPO Center, which is an accredited CEDRP dispute resolution provider.

110. Up-front verification limits the likelihood of cybersquatting, although it cannot completely exclude it. Since the sponsored gTLDs do not require applicants to establish a connection to the desired domain name, it is still possible for members of the concerned group to register domain names in violation of trademark rights of others. It is mainly for this reason that the UDRP also applies to sponsored gTLDs. Until now, there is however no evidence of cybersquatting relating to these TLDs. By the end of 2004, only one UDRP case filed with the WIPO Center concerned a sponsored name.[64] The case involved the domain name <aeroturbine.aero> and concerned a dispute between conflicting right holders in the aviation industry. A three-member panel found that the respondent had a legitimate interest in the domain name and dismissed the complaint.

111. The New gTLDs Report found that the verification mechanisms adopted by these sponsored gTLDs worked reasonably well, and that none of these gTLDs have become havens for cybersquatting or other registration abuses.[65] On the other hand, the study made the following recommendation:

> "ICANN might wish to review whether there are technical or policy considerations that would justify limiting registrations in a sponsored gTLD to registrants that can establish a connection to the desired domain name. Such a change would be more relevant for .aero and .coop than for .museum, where there is already a strong nexus between registrants and their registrations. Some of the differences between an unsponsored and a sponsored gTLD might support such a policy distinction. On the other hand, such a requirement could discourage multiple registrations in registries where the number of registrations is already lower than expected. Perhaps most important, it could be difficult for a sponsored gTLD to make the kinds of subjective and potentially intrusive decisions that might be required to enforce such a policy."

112. Form an IP perspective, the sponsored gTLDs that have been introduced so far have given little cause for concern. The up-front verification of domain name applications limit the range of potential registrants and increase the cost of registrations. Because of their narrow scope these gTLDs may have limited commercial appeal beyond the sponsored community. These factors reduce the likelihood of cybersquatting, although they cannot completely exclude it. Should cybersquatting occur, it can be addressed under the UDRP.

---

64 WIPO Case No. D2004-0669, *AeroTurbine, Inc. v. Aero Turbine, Inc.*, October 27, 2004.

65 Report on Compliance by Sponsored gTLDs with the Registration Requirements of Their Charters published on February 25, 2003; available at *http://www.icann.org/committees/ntepptf/stld-compliance-report-25feb03.htm*.

8. Conclusions: IP Protection in a Start-Up Scenario

113. As stated earlier, this document does not address the fundamental question as to whether there should be further new gTLDs. Instead, it attempts to provide guidance on the means of protecting IP when a new gTLD is introduced. The above analysis has shown that the start-up of a new gTLD raises a number of challenges for curative as well as preventive IP protection.

8.1 Curative Protection: the UDRP and New gTLDs

114. The strength of the UDRP lies in its proven efficiency as a means to provide relief against the abusive registration of domain names that correspond to trademarks. In addition, the UDRP takes account of the rights or legitimate interests a holder may have in the disputed domain name. The stable, and recently even increasing, number of cases under the UDRP suggests, however, that it cannot completely exclude cybersquatting.

115. In a start-up scenario, the curative efficiency of the UDRP is limited since, as currently worded, it requires a trademark owner to prove registration **and** use in bad faith. Following the introduction of a new gTLD there may have been little occasion to use a newly registered domain name. This may hinder obtaining curative relief where it is urgently needed. One way to address this limitation could consist in amending the UDRP to require proof of registration **or** use in bad faith, as was done in STOP which applied to certain start-up conflicts in .biz (see above). Such an amendment would also facilitate the application of the UDRP to new domain name registrations in existing gTLDs, all the more so since some bad faith respondents may deliberately abstain from using a domain name.[66] The experience in .biz shows, however, that, even with such an amendment, the UDRP will provide efficient relief in a start-up scenario only to well-known marks. This should, however, be the result of a conscious policy decision, rather than the unforeseen consequence of a default choice.

8.2 The Need for Preventive IP Protection

116. One of the most important questions to be addressed when a new gTLD is introduced is whether all, or at least certain types of, IP owners should enjoy some form of preferential treatment in the attribution of domain names over members of the general public, or whether they should, like everyone else, compete for their names in a (randomized or first-come first-served) assignment procedure. Phrased differently, the question is whether a new gTLD should provide preventive IP protection mechanisms, or whether curative mechanisms, such as the UDRP, provide sufficient protection. Experience suggests that the need for such

---

[66] Since the adoption of the UDRP, a number of ccTLDs, including .au, .ie, and .ir, have adopted dispute resolution policies that follow this approach. In light of the experience gained under, and reactions to, the UDRP, such an amendment would now appear relatively uncontroversial.

preventive mechanisms depends in large part on type of the gTLD to be introduced, and the resulting degree of attractiveness for cybersquatters.

117. Curative mechanisms may suffice when a new gTLD is subject to clearly circumscribed, verified and enforceable registration restrictions. Preventive protection mechanisms may be necessary where right owners are likely to resort to preemptive practices in order to prevent cybersquatting, confusion and dilution and are prepared to bear the resulting cost. It is hard to assess when exactly this will be the case. Neither the number of Sunrise registrations in .info, which was due to the large share of non-compliant registrations, nor the number of IP Claims filed in .biz, which may have been inflated by incentives to file multiple claims, provide conclusive indications. As stated above, the need for preventive protection will be more tangible in the following three types of gTLDs:

(i) completely unrestricted or "open" gTLDs, such as .info;

(ii) gTLDs with minimal or nominal restrictions such as .biz, which is open for any "*bona fide* business or commercial use";

(iii) gTLDs with geographic rather than subject matter restrictions, such as the proposed new sponsored gTLD .asia for the "Pan-Asia and Asia Pacific community".[67]

8.3 Preventive IP Protection Mechanisms

118. The experience gained thus far suggests that preventive IP protection mechanisms should satisfy (at least) the following requirements:

(i) Protection mechanisms should be effective in order to prevent new gTLDs from turning into cybersquatting havens, which would not only damage the interests of IP owners, but also the reputation and credibility of the gTLDs in question;

(ii) Protection mechanisms should be designed in a way that minimizes the potential for abuse. The more a mechanism is open to abuse, the less credibility and legitimacy it will have, and the less it can serve its purpose;

(iii) Protection should be balanced and take account of rights and interests of third parties wherever this is reasonably feasible;

(iv) The protection mechanism should be practicable and not overly complex, and should not cause undue delays in the introduction or functioning of the gTLD as a whole.

---

[67] See the .asia New sTLD RFP Application, *http://www.icann.org/tlds/stld-apps-19mar04/asia.htm.*

119. So far, the following preventive protection models can be identified:

(i) Watch services, possibly combined with preferential options to initiate a dispute resolution procedure against abusive registrations;

(ii) Defensive registrations, possibly combined with a preferential registration period;

(iii) Exclusion mechanisms, as suggested in the First WIPO Report;

(iv) Sunrise mechanisms that allow right holders to register domain names corresponding to their IP rights before the general public.

120. *(i) Watch services.* Watch services, whether or not combined with additional options, have some benefits: they offer hardly any incentive for abuse, do not interfere with potential legitimate interests of domain name applicants and holders and, since they can be operated in parallel with the general opening of the gTLD, do not delay its introduction. On the other hand, while costly to rights owners, they are of limited efficiency in preventing abuse since they mainly serve to facilitate curative relief, which would have to be obtained for example through court litigation or under the UDRP. The rate of abandoned domain name applications in .biz seems to suggest, however, that a watch service can also have some preventive effect if domain name applicants are notified of any conflicting claims before registering the name they applied for.[68]

121. Determined cybersquatters will however not easily be dissuaded by such warnings. IP owners are therefore likely to seek more tangible means of preventing abuse and will therefore try to register their most valuable identifiers as domain names. This, in turn, will further increase the cost for rights owners. Hence, it appears doubtful whether such a system justifies the costs resulting from its establishment and operation, and the fees to be paid by rights owners. The experience with STOP has shown, moreover, that a preferential option to initiate a dispute resolution procedure, which would be subject to yet another fee, will provide effective curative relief mostly to holders of well-known marks only.

122. *(ii) Defensive Registrations.* Defensive registrations seem particularly appropriate in restricted gTLDs where right owners may not be eligible to register domain names (and can therefore not use any Sunrise registration possibility offered), but may still wish to prevent abuse directed at their rights.[69] This may be the case in particular where the TLD in question addresses a wide audience, such as a sponsored or restricted gTLD with minimal subject matter restrictions. Since defensive registrations block registrations by others, their

---

[68] The applicant for the sponsored TLD .xxx suggests to establish "the STOP proceeding as originally implemented by NeuLevel during the launch of the .biz TLD", New sTLD RFP Application .xxx, posted at *http://www.icann.org/tlds/stld-apps-19mar04/xxx.htm*

[69] The applicant for the sponsored TLD .cat suggests to provide defensive registrations to "registered trademark owners who do not comply with the eligibility criteria and do not belong to the sponsored community", see .cat New sTLD RFP Application, *http://www.icann.org/tlds/stld-apps-19mar04/cat.htm*.

preventive efficiency is high. In order to prevent cybersquatting during start-up, defensive registrations could be made available to right owners during a Sunrise period, i.e., before the general public can file domain name applications. Abuse of the defensive registration option is somewhat less likely because it cannot be used to attract Internet traffic; abuse could be prevented if the trademark credentials of applicants were verified before registration, and third parties could challenge non-compliant defensive registrations. As in .name, domain name applicants whose application is blocked by a defensive registration could be enabled to overcome this blocking effect by proving their eligibility to register a name. As in .name, this will, however, significantly increase the system's complexity.

123. *(iii) Exclusion Mechanisms.* Since no exclusion mechanism has been implemented yet, it is not possible to assess its practical effects. Its strength would lie in the fact that, as suggested, it would be centralized and provide effective defensive protection across all (open) gTLDs. Unlike in a Sunrise mechanism, rights owners would therefore not need to register and maintain (potentially large) portfolios of preemptive domain name registrations in different gTLDs. Its scope would normally be limited to well-known marks, the type of marks which enjoy a higher degree of protection under international law and is most likely to attract cybersquatting. However, since it is not easy to determine whether a given mark is well known, the mechanism would require the establishment of an administrative procedure with a network of neutral trademark experts deciding on applications. As a result, the cost of the mechanism would likely be comparable to that of a UDRP procedure. The introduction of new gTLDs would not be delayed since only names for which an exclusion was requested would be blocked pending verification, while the remaining domain name applications could proceed.

124. *(iv) Sunrise Mechanisms.* There seems to be a clear trend among TLDs towards Sunrise mechanisms as a means to protect the interests of IP owners. In addition to .info, a number of ccTLDs that liberalized their registration conditions (such as .in, .kr, .sg or .us) or TLDs that are about to open (such as .eu) have adopted such preferential registration options. Some of the recent applicants for new sponsored gTLDs (.asia, .cat, .mobi, .tel), also propose Sunrise periods for rights owners.[70] One reason for this trend may lie in the fact that Sunrise mechanisms offer the most tangible benefit to right holders, the domain name itself, even if it may be burdensome for rights owners to acquire and maintain large domain name portfolios in different gTLDs.

125. As stated above, however, in restricted or sponsored gTLDs, a Sunrise period will only protect the interests of rights owners who are eligible to register in the concerned gTLD. This may be sufficient where the gTLD in question is restricted to clearly specified and narrowly circumscribed purposes because the potential for conflict is limited. The wider the audience that is addressed by the gTLD, the bigger the need for additional preventive measures, which, in such cases, could be provided by also offering defensive registrations.

---

[70] All applications are posted at *http://www.icann.org/tlds/stld-apps-19mar04/stld-public-comments.htm.*

126. The following paragraphs summarize the key elements of any Sunrise mechanism: its scope and the need for, and viability of, mechanisms to verify compliance with Sunrise eligibility criteria.

127. *Scope.* As far as its scope is concerned, Sunrise mechanisms could

(i) be made available to owners of any type of protected identifier,

(ii) be limited to registered trademarks, or

(iii) be limited to well-known marks.

128. If Sunrise registrations were available to all owners of rights in identifiers (trademarks, trade names, personal names, geographical indications, names and acronyms of IGOs, etc.), all owners of such rights would compete during Sunrise on an equal footing. This seems to be the current legal situation in most jurisdictions. The problems with such an approach, however, are twofold: first, not all these types of rights are recognized in every jurisdiction while a gTLD would normally have to take a global approach and could hardly take account of such limitations; secondly, the verification process will be complicated by the inclusion of unregistered rights, such as unregistered trademarks and trade names. It would therefore seem justified to restrict the Sunrise option in a gTLD to rights that have a clear basis in international law, and that are subject to registration mechanisms. This would include at least trademarks and the names and acronyms of intergovernmental organizations (IGOs). Both are protected under the Paris Convention as well as the TRIPS Agreement. Trademarks can be registered at the national or (as for example in the case of the EU) regional level; names and acronyms of IGOs are registered centrally with WIPO pursuant to Article 6*ter* of the Paris Convention.[71] In order to take account of the high degree of support voiced in the Second WIPO Internet Domain Name Process for the protection of country names (as represented in the UN Terminology Bulletin), these identifiers could also be covered by Sunrise mechanisms.

129. The Sunrise mechanisms that have been implemented so far have, for practical reasons, been limited to registered trademarks. Such rights exist in almost every jurisdiction and can be proved and verified on the basis of official trademark certificates and, in some cases, online databases. As explained above,[72] two further conditions were applied, which gave rise to certain problems: first, it was required that the trademark be registered before a certain cut-off date, presumably in order to prevent that trademarks are registered purely with the intent to obtain a certain domain name before the general public. From an IP perspective it would seem more logical to require that a certain mark had been applied for before a certain date, provided that it was registered prior to the start of the Sunrise period. Secondly, the domain name had to be identical to the textual or word elements of the trademark registration. This enabled holders of marks, which consisted of generic terms but could be registered because of

---

71 Further information about this mechanism is available at *http://www.wipo.int/article6ter/en/*

72 See paragraphs 73-74.

distinctive ornamental or scriptural features, to secure domain names corresponding to the non-distinctive word elements of their mark, although these elements did not enjoy trademark protection as such. If a Sunrise mechanism is limited to registered marks, one might consider limiting it even further to word marks.

130. Some criticize Sunrise mechanisms for giving IP owners broader rights than they enjoy in the real world because an IP owner who has been able to register a name before the general public blocks this name for other uses, including legitimate ones. In response to such concerns, the First WIPO Report suggested to limit the exclusion mechanism (described above) to marks that are well known across a widespread geographical area and across different classes of goods and services because such marks enjoy a higher degree of protection under international laws than other types of IP rights. Limiting Sunrise mechanisms to owners of such rights may avoid such criticism.

131. Such a limitation would, however, require a fairly sophisticated verification (and challenge) mechanism. It is far easier to determine whether a trademark has been registered in a certain jurisdiction than it is to determine whether a mark is well known. For this reason, the First WIPO Report suggested a procedure in which this assessment would be carried out by a panel of independent trademark experts on the basis of material submitted by the applicant.

132. *Verification.* The .info experience shows that Sunrise mechanisms should include some form of up-front verification.[73] The possibility of filing applications before the general public constitutes a significant advantage that should not be made available in a manner that can easily be abused. Widespread abuse would undermine the legitimacy of the Sunrise option as a means to protect owners of rights in certain identifiers; it can also be harmful to rights owners whose identifiers may be taken by non-compliant registrants. Verification should cover all Sunrise registrations and preferably be performed by a neutral third party as a condition for releasing the name to the registrant.

133. The .info experience also demonstrates that *ex post* mechanisms, such as Sunrise Challenges, cannot substitute up-front verification. Experience with the .info Sunrise mechanism suggests that third parties will only have an incentive to file challenges if they have a chance of obtaining the name for themselves. This may leave many names that were registered in violation of the Sunrise conditions unchallenged because no other party owns rights in these terms; this concerns in particular generic or descriptive terms, which often are among the most attractive and valuable domain names. Sunrise challenges may nevertheless constitute a useful supplement to address violations of the Sunrise conditions that either were not caught during verification or that occurred later, for example when a domain name is transferred to an ineligible third party. As in .info, they could provide a process for the registry operator to cancel non-compliant domain name registrations.

---

[73] This recommendation has already been made earlier, see, e.g., WIPO .INFO Report, Annex 1, page 1; WIPO STOP Report, page 14.

134. The New gTLDs Report suggests that verification is feasible:

> "First, the availability of online trademark databases makes verification a more manageable task than at first may be apparent.[...] There is no question that verifying trademark claims in the context of launching a global product is challenging. Trademark registration processes and accessibility to relevant information varies among countries. On the other hand, several of the world's largest trademark databases are online, with the highest such concentrations in North America and Europe. There were 49,285 (95.2%) out of 51,764 .info Sunrise registrations that came from these two regions, which suggests that a properly designed program could have therefore verified the vast majority of submissions without great difficulty. For the .us ccTLD, for example, NeuStar designed a system to verify trademark submissions against the U.S. Patent & Trademark Office database during launch of .us. Reports indicate that the system worked well. Verifying registrants in a global database is obviously more complicated, but the example illustrates the possibilities afforded by access to online databases. There would of course still need to be some manual review to address any questions and to deal with databases that are not accessible.
>
> "Second, the cost of verification need not be prohibitive if it is distributed among all Sunrise registrants. Verifying trademark submissions is not an inexpensive proposition, but Afilias discovered that the cost of fixing problems later can be high. The primary cost factor to consider is whether verification can be done on the basis of an online database or not. Other factors to weigh include: (i) the number of verifications anticipated and thus the number of staff needed; (ii) the timeframe for verification; (iii) the costs of staff and overhead of the entity performing verification; (iv) the substance of the registration standard and any processing requirements; (v) the amount of staff training required; (vi) the number of queries expected from actual or potential registrants; and (vii) any infrastructure investment needed to build or maintain the verification database. Rough estimates for checking online databases range from $10 to $30, but could be lower if the process is fully automated. Estimates of the expense of checking databases that are not easily accessible run higher, and tend to start at around $300. Rather than impose a two-tiered pricing schedule, which people thought would be too complicated to administer and could be unfair to trademark holders in jurisdictions requiring manual verification, particularly in developing regions, use of cost averaging could establish a fee that would cover the cost of checking both situations.[...] Interviews with members of the intellectual property community indicated that they would not object to paying reasonable costs directly related to the cost of running a verification program, as long as they were not assessed a premium for protecting their rights. This view is consistent with those of other end-users, who felt that trademark holders seeking the benefit of registration ahead of the general public should have to pay any associated costs."[74]

135. Following the .info experience, the TLDs that offered, or plan to offer, a Sunrise mechanism all provide for up-front verification. The verification can at least partly be automated with regard to holders of trademarks registered in jurisdictions which have an

---

[74] New gTLDs Report, page 24-25.

online trademark database, although the programming time and cost should not be underestimated, in particular since the format of databases may differ from country to country.[75] While ccTLDs, such as .us, may be in a position to limit the Sunrise option to rights registered in one jurisdiction which offers a searchable online database, this is not an option for gTLDs which address a potentially global public and will therefore be required to accept rights registered in any jurisdiction, including those which do not offer online databases.

136. Verification will be complicated if holders of unregistered rights, such as unregistered trademarks or trade names, are also made eligible to obtain Sunrise registrations. This is the case for .eu, which has therefore developed probably the most complex Sunrise mechanism so far. The .eu TLD plans to offer a "phased registration" possibility to all holders of national or Community-wide rights in signs. To deal with the resulting complexities, there will be two Sunrise periods: during the first period, only holders of rights that can be verified more easily are eligible to apply; this includes registered national and Community trademarks, geographical indications, and the names and acronyms of public bodies. During the second stage, unregistered trademarks, trade names, business identifiers, company names, family names, and distinctive titles of protected literary and artistic works may also be registered.[76] Applications can be based on any right recognized in any EU Member State and will be verified by neutral expert "Validation Agents". Supporting material can be submitted in any EU-language. Decisions of Validation Agents can be appealed to a neutral panel of experts in an ADR procedure.[77] Until an application for a name is accepted or until all applications for that name are rejected, the domain name in question will be blocked from being registered by any other party, even if validation has not taken place by the time open registration begins.

137. The costs of any verification mechanism will also depend on its scope. Such costs may include the costs for setting up and operating an IT system to check trademark data against different national and regional databases, the costs of checking trademark certificates in countries that have no online register, and, potentially, the cost of verifying unregistered rights. It seems justified that the costs of reasonable verification mechanisms be covered by its beneficiaries, i.e. the applicants. As a result, the Sunrise fees will be higher than those charged for "normal" domain name applications. To a certain extent this may also serve to discourage domain name speculators.

---

75 WIPO provides a Trademark Database Portal with links to online trademark databases established by national or regional trademark offices at *http://arbiter.wipo.int/trademark.*

76 Article 12.2 Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration, Official Journal of the European Union No. L 162/40 of 30.4.2004, also available at *http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_162/l_16220040430en00400050.pdf.*

77 Article 22.1(b) Commission Regulation No. 874/2004.

8.4 Clarity and Cooperation

138. One of the key lessons of the first expansion of the DNS is the need for clarity and cooperation among the various actors involved. As a result of ICANN's experimental "proof of concept" approach, several different gTLDs with different registration restrictions and different IP protection mechanisms were introduced. This caused a fair deal of confusion among registrars and domain name registrants, including IP owners wishing to protect their rights. IP protection mechanisms can only achieve their purpose if the mechanism is clearly structured, not overly complex, and if all participants are well instructed and prepared to cooperate. This would also require ICANN to exercise a supervisory function by monitoring compliance of individual gTLD operators with the relevant terms of their accreditation agreements, relating to issues such as the maintenance of a reliable Whois registry, compliance with registration restrictions, implementation of up-front verification mechanisms, and implementation of decisions rendered in the context of a dispute resolution policy applicable to the gTLD in question.

8.5 A Uniform Preventive IP Protection Mechanism

139. Regardless of the comparative benefits and disadvantages of each of the mechanisms discussed in the preceding paragraphs, a further helpful reduction in complexity could be achieved if a uniform mechanism were adopted. The UDRP provides a good example of a uniform mechanism that works efficiently across different gTLDs. While less tested in practice, the CEDRP is another uniform dispute resolution mechanism. A similar degree of uniformity would certainly be helpful with regard to preventive introductory IP protection mechanisms (as suggested in the First WIPO Report):

- Operators of new gTLDs would not be required to develop and implement their own IP protection mechanisms, a task for which they are not necessarily equipped;

- ICANN would not be required to monitor the correct implementation of multiple protection mechanisms applied by different gTLDs, but could concentrate its attention on one single mechanism;

- IP owners would not be required to devote significant resources to understanding multiple different IP protection mechanisms.

140. The mechanism could either be applicable in new open gTLDs only, or applied uniformly across all new gTLDs that may be introduced over time, including restricted and sponsored gTLDs. As stated earlier,[78] there may also be need for preventive protection in certain types of restricted or sponsored gTLDs. A truly uniform approach would have the

---

[78] See paragraph 117 above.

advantage of avoiding difficult distinctions between "really open" and "sufficiently restricted/sponsored" gTLDs, without however overly burdening the introduction of restricted or sponsored gTLDs since their operators would not be required to develop and implement the mechanism themselves.

141. In view of the trend towards Sunrise mechanisms, a uniform mechanism of this type could be developed. New gTLDs would be required to offer IP owners the option of registering their protected identifiers during a Sunrise period of a specified duration before they accept registrations from the general public. In sponsored or restricted gTLDs where IP owners may not be eligible to register domain names, they could instead be given the option of obtaining defensive registrations during the Sunrise period. When developing such a mechanism, particular attention will have to be given to the structural key elements of Sunrise mechanisms which have been outline above.[79]

142. Adopting and implementing a uniform mechanism would appear to be a logical conclusion from the "proof of concept approach" adopted by ICANN in the first introduction of new gTLDs. The experience gained in this context, and in the five years of successful operations under the UDRP, provide sufficient guidance for introducing a uniform preventive IP protection mechanism that could apply across all new gTLDs.

[End of document]

[79] See paragraphs 127-137 above.