

CHAPTER 8

DOMAIN NAMES: A GLOBAL VIEW

Fredrik Roos
Setterwalls
Göteborg, Sweden

8.01 Introduction

This chapter will provide an overview of the evolution of the Domain Name System and related legal issues, including the set of rules regulating the issuance of domain names and the resolution of disputes regarding domain names. The most important concerns will be discussed, and references will be provided to more specialized work for deeper studies.

This chapter also will provide a global perspective of the Domain Name System, discussing the importance of cultural differences, the role of Country Code Top Level Domains, the division of the Internet into different languages, and the need for the harmonization of systems for dispute resolution.

8.02 The Domain Name System

(a) What are Domain Names?

Every computer connected to the Internet has an individual numerical address, referred to as an “IP Number”, which enables a message from one computer to another to find its way on the Internet. The IP Numbers are naturally too difficult for a human being to memorize. We are more used to remembering addresses in the form of words and, therefore, a system that translates the IP Numbers into words has been created, the domain name system.

A typical domain name consists of a main-domain located in a top-domain and sub-domains attached to the main-domain. The appearance in an Internet browser window is sub-domain.main-domain.top-domain. An

example is the address of my former department at the University “informatics.gu.se”. Top-domains can be either generic, e.g., “.com”, or belong to a country, e.g., “.se” and are often referred to as Top-Level-Domains (TLDs). The main-domain name usually leads to the homepage,¹ of a website² such as “gu” (Gothenburg University), and then sub-domains are linked to the homepage, such as “informatics” (the Department of Informatics).

(b) Purpose of Trade Marks and Domain Names

Since the domain name is the address that enables people to find other people, companies, or organizations, it is very important. Today, there are more than 16 million “.com” domains, and this large interest alone proves its importance as an asset. However, what is of real importance is not just having a domain name, but rather that the domain name is a good one.

A good domain name is intuitive, easy to remember, and likely to be noticed on the Internet. For businesses, the commercial importance of domain names as trade marks can be tremendous.³ The right to a domain name has become a form of proprietary brand asset. This right can provide a competitive advantage that contributes to the equity of the brand.⁴ If the brand is already used as a trade mark, it is of great importance to the trade mark holder to also have the right to the domain name.

The Domain Name System (the “DNS”) requires everyone on the Internet to have a unique domain name address; however, different companies in different countries, or different kinds of businesses, have similar or identical trade marks.

Previously, this has not been a problem since domains have not been competing for the same customers but, with the creation of the DNS and the widespread use of the Internet, potential conflicts have sprung up over the use of the same domain name. In conjunction with this are other related problems involving the DNS and trade mark law, in particular the practice of cybersquatting (acquiring a domain name and trying to sell it to the rightful owner).

(c) Evolution of the Domain Name System

(i) ICANN

To regulate policy for the DNS, the United States government proposed the creation of a not-for-profit entity based in the United States. This entity

1 “Homepage” is used here as the definition of the “first page” of a website, the page one is expected to first arrive to, as in “cocacola.com” or “microsoft.com”.

2 “Website” is used here as the definition of a set of linked web pages belonging to, e.g., a company or an organization.

3 Lindqvist, “Domännamn — stöld, strategi och utveckling”, *Centraltryckeriet* (1999).

4 Aaker, *Building Strong Brands*, at pp. 7–9 (1996).

would be devoted to the collective interest of the Internet as a whole, with a board to be composed of representatives of stakeholders on the Internet and charged with authenticating the policy decisions that the Internet Assigned Names Authority (IANA) was to make. In exchange, the United States government would give up the administration of the DNS and instead support the delegation in its transition to the Internet Corporation for Assigned Names and numbers (ICANN).

At the time, the creation of ICANN seemed a logical and obvious choice. A private entity would take up the tasks of the government, but it would not be the government *per se*. Nevertheless, almost five years after its creation, there are accusations that the corporation has failed to implement the principles and structures that would turn it into an e-government and that its role in relation to Internet governance, especially towards citizens and their rights, is rather ambiguous.

(ii) *History of ICANN*

From 1994 to 1998, a series of attempts to move Internet administration into the private sector were made. The attempts began with the Internet Society (ISOC) in the United States, but gradually escalated as the ISOC realized that allies were needed to help it carry out this agenda.⁵

Prior to ICANN's creation, a string of authorities, corporations, and companies were responsible for the administration of the DNS; however, all of these authorities were directly or indirectly contingent on the intervention of and approval by the United States Department of Commerce. While the Internet was evolving and turning into a global medium, many governments around the world started questioning the United States government's influence and control of this exceptional interchange.

In June 1998, the United States Department of Commerce released a White Paper on the administration of Internet names and numbers, the ostensible purpose of which was to reposition the management of Internet domain names and IP addresses out from under the influence of the United States federal government and into the hands of a private, non-profit organization with international participation and representation.⁶ In November 1998, the United States Department of Commerce officially recognized ICANN as the organization responsible for the administration and supervision of the domain name system.⁷

5 Mueller, "ICANN and Internet Governance: Sorting through the Debris of "Self-Regulation", *Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, volume 1, number 6 (December 1999).

6 Department of Commerce, NTIA, "Management of Internet Names and Addresses", *Statement of Policy, Federal Register*, volume 63, number 111 (10 June 1998), at p. 31741.

7 See <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>.

To justify this transmission and ease the concerns surrounding such an action, the United States Department of Commerce decided to adopt the “self-regulatory” model, a concept already tested and approved by other industry sectors. “Self-regulation” meant that the United States government would not be involved in the creation of the new organization or specifically define its power and structure.

Instead, it invited the private sector to form an entity that would be based on a broad consensus among industry stakeholders. Once the “private sector” came to the government with a formal proposal, the latter would delegate its assets and, after two years of supervision, the United States government would walk away. That, at any rate, was what was supposed to happen.

“Self-regulation” had been a *leitmotif* of other Clinton Administration efforts to privatize sectors of the digital economy; it characterized its approach to digital television broadcasting,⁸ the protection of online privacy,⁹ and content regulation.¹⁰ “Self-regulation” also was a term easily affixed to the Internet itself, and it resonated rhetorically with the culture of the Internet’s engineering and technical community, which needed to be convinced of the success of the process.

During the period that the United States Department of Commerce was drafting the White Paper that would eventually pave the way for ICANN’s debut, ICANN started making its first moves. First, it laid down its bylaws and determined its board of directors while, at the same time, making clear to the other existing organizations that it would take up their tasks and would be the sole administrator of the Internet. As a result, as soon as ICANN was officially launched, the chores of the ISOC, IANA, and Network Solutions, Inc. (NSI) were incorporated into ICANN’s duties.

Second, and occurring concurrently, while trade mark owners were pushing for the lion’s share on the Internet, ICANN, instructed by the White Paper, asked the World Intellectual Property Organization (WIPO) to devise a

8 In December 1998, an Advisory Committee on Public Interest Obligations for Advanced Television recommended that the National Association of Broadcasters, acting as the representative of the broadcasting industry, draft an updated voluntary Code of Conduct to highlight and reinforce the public interest commitments of broadcasters, at <http://www.benton.org/PIAC/>.

9 The United States Department of Commerce, along with the Office of Management and Budget, was asked to report to President Clinton on industry efforts to establish self-regulatory regimes to ensure privacy online and to develop technological solutions to protect privacy. This led to its staff discussion paper, “Elements of effective self regulation for protection of privacy”, at <http://www.ntia.doc.gov/ntiahome/privacy/index.html>.

10 The United States government has passed legislation to install the “V-chi” and associated ratings systems in televisions and has encouraged the development of the Platform for Internet Content Selection (PICS) standard for Internet content.

dispute resolution procedure that would assist in resolving the conflicts between trade marks and domain names. After a period of consultation and debate, ICANN introduced the Uniform Domain Name Dispute Resolution Policy (UDRP) to the trade mark world.

ICANN's creation served two main purposes. The first one was to take the Internet out of the realm of United States domination and governmental control, and the second was to satisfy the desires and wishes of citizens. The tasks that ICANN was requested to carry out were specified in the White Paper. One of the principal catalysts behind the launching of ICANN was the need to de-monopolize the business of registering domain names.¹¹ Before ICANN's creation, Network Solutions, Inc. (NSI) was the sole registrar and had a *de facto* monopoly of all registrations in the generic Top Level Domains (gTLDs), based on its contract with the United States government. The purpose of ICANN's formation was to eliminate the NSI monopoly and allow other registrars to enter the market, thus stimulating competition.

A second task ICANN had to undertake was the formulation of a dispute resolution policy for potential conflicts between trade marks and domain names. The pre-existing policies had many deficiencies, and a number of citizens, the trade mark owners, were seriously dissatisfied. Consequently, one of the first concerns of ICANN was to somehow manage to satisfy two diverse groups of citizens: trade mark owners and domain name holders. Based on recommendations from WIPO, ICANN produced the Uniform Domain Name Dispute Resolution Policy, which allows conflicting parties, regardless of which jurisdiction they may operate under, to settle their disputes through a form of quasi-arbitration, thus providing an alternative option to the courts.

Moreover, ICANN took on board Jon Postel, the original creator of the DNS. In accordance with Postel's suggestions, ICANN introduced the country code Top Level Domain Names (ccTLDs).¹² Postel had made it clear from the beginning that, when it comes to ccTLDs, there should be no policy involved as the Internet community is not in a position to define what a country is or recognize a territory or other geographic unit as a "country".¹³ ICANN's job in this case was to ensure that all ccTLDs are properly added to the authoritative root and thus enable all websites using ccTLDs to be visible on the World Wide Web (WWW).

11 Kleinwaechter, "Governance Systems in the Internet Age: ICANN between Technical Mandate and Political Challenges", at <http://www.mcc.ruc.dk/aktuelt/2000/symp/kleinwaechter-paper.pdf>.

12 Yu, "The Neverending ccTLD Story", *Public Law & Legal Theory Working Paper Series*, Research Paper Number 1-22, at <http://ssrn.com/abstract=388980>.

13 Kleinwaechter, "Governance Systems in the Internet Age: ICANN between Technical Mandate and Political Challenges", at <http://www.mcc.ruc.dk/aktuelt/2000/symp/kleinwaechter-paper.pdf>.

(iii) CcTLDs

Since no policy was created for the ccTLDs, their delegation became somewhat arbitrary. In many western countries, university employees introduced the Internet, and at that time they were organized into different not-for-profit Internet organizations; consequently, the governments' knowledge of the Internet was very limited. As a result, the control of the ccTLD was in many cases delegated to the not-for-profit organizations. In less technologically developed countries, the control over the ccTLD was generally delegated to the government, where it was not actively used until years later.

The not-for-profit organizations operated under the fundamental principle that “the net should be free”. However, in the second half of the 1990s, the Internet began to be commercialized, and not only by universities and enthusiasts, but companies, consumers, and individuals began to take an interest in domain names.

(d) Need for Regulation of the Domain Name System

The *laissez-faire* concept of an open market with many companies competing to establish themselves is one whose practical application has not always proven itself feasible. There are examples of scarce resources or instances where a form of direction and regulation has been required. The DNS is a classic example. It has a strict hierarchical structure and, as of yet, there is no technical way to administer it without this hierarchy.

The domain names in a TLD must be unique. Subsequently, two different interests may both have a legitimate claim to the name, or alternatively one of them may have a more illegitimate motivation, such as the wish to extort others who wish to use the name (cybersquatting); yet, in either instance, they will still be able to register the name in a TLD. Both situations will obviously result in disputes; the only solution — someone must regulate the DNS. Some TLDs have chosen to regulate the issuance of domain names, while others have decided to create an independent mechanism for the purposes of arbitrating conflicts.

8.03 Issuance of Domain Names and Related Conflicts**(a) Issuance of Domain Names***(i) First Come, First Served*

The control of the majority of the TLDs is very liberal, and the “First come, first served” principle is generally applied to the issuance of domain names, i.e., the registration of a requested domain name is granted provided that the name is not already registered. ICANN applies the “first come, first served”

principle to the generic top-level domains (gTLDs),¹⁴ as is done with the German and United Kingdom TLDs.

That a country applies the “first come, first served” principle does not necessarily mean that the domain is completely available for registration. Many TLDs require the applicant to have a relation to the ccTLD, i.e., that they be a company, organization, or individual who is a resident in that country. Other restrictions include reserved names that for different reasons are not allowed to be registered as domain names.

An example is the Canadian TLD “.ca”, which requires having a “Canadian Presence” to register a domain name, i.e., the applicant must be an individual or an organization with a connection to Canada (a Canadian citizen, corporation, or organization).¹⁵ The German “.de”, on the other hand, is an example of the more liberally controlled TLDs. To be allowed to register a domain name in Germany, the applicant is only required to have a contact person in Germany.¹⁶

(ii) Rules for Registration

Another attempt has been to control ccTLDs by applying more detailed rules to the registration of domain names. These systems typically require the applicant to have not only a connection to the relevant ccTLD, but also some form of documented connection to the specific domain name applied for. An example of such a documented connection is that the domain name is identical or very similar to a registered company name or trade mark held by the applicant.

The application of such rules for registration is an attempt to achieve a certain standard of registered domain names in the ccTLD and assure that the ccTLD is used in the desired way. The purpose being to ensure that what is published under a ccTLD is representative of, or at least has a connection with, the country related to the ccTLD.

The rules for registration have served their purpose well. TLDs applying such rules have traditionally had little or no problems with disputes (e.g., trade marks) concerning domain names. Consequently, there has been no need for an alternate dispute resolution system. The registered domain names also have been almost exclusively used by companies and organizations with a strong connection to the country related to the ccTLD.

However, there is a built-in problem with these systems based on the difficulty in registering domain names. Systems requiring that a domain name

14 Bryde-Andersen, *IT-retten*, avsnitt 11.5.c (2001).

15 CIRA Registration Rules, Version 2.2, at <http://www.cira.ca>.

16 See <http://www.denic.de/de/bedingungen.html>.

must reflect the exact registered name of a company exclude not only trade marks, personal names, and abbreviations of long or difficult company names, but also generic names as domain names. It is self-evident that every company and individual that is not granted the registration of a desired domain name will question the system.

Consequently, an international trend has been that the rules for registration have changed from being very restrictive to very accessible. They have undergone a liberalization process that started with allowing each company to register an unlimited number of domain names corresponding to the abbreviations of the company name and any registered trade marks. In recent years, many ccTLDs have taken the full step toward liberalization and implemented the first-to-file system. These ccTLDs include:

1. The Belgian “.be”;
2. The Dutch “.nl”;
3. The French “.fr”;¹⁷
4. The Greek “.gr”;
5. The Irish “.ie”;
6. The Luxembourgian “.lu”;
7. The Norwegian “.no”;¹⁸ and
8. The Swedish “.se”.¹⁹

Another instigator behind the push for liberalization was that the rules for registration proved to restrain the popularity of a ccTLD, thereby causing a country’s inhabitants and companies to register their domain names in other countries’ ccTLDs or a gTLD, in effect counteracting the original purpose of applying these rules to create a ccTLD that was the natural domicile for the country’s inhabitants and companies. Compounding this, of course, was the resultant loss of profit due to the relatively small number of registered domain names.

A striking example is the French ccTLD “.fr”. Prior to liberalization, it had only 160,000 registered domain names.²⁰ Compare this with the German “.de”, with more than 7-million registered names,²¹ or the Danish “.dk”, with 450,000 registered domain names. France has more than 10 times the

17 See <http://www.nic.fr>.

18 See <http://www.norid.no/>.

19 Roos “‘First Come, Not Served’: Domain Name Regulation in Sweden”, *International Review of Law Computers & Technology*, volume 17, number 1 (2003).

20 See www.nic.fr/statistiques/afnic/afnic-repart.html.

21 See www.denic.de/DENICdb/stats/index.en.html#domaincount.

population of Denmark and an approximately comparative level of information technology development, yet the Danish ccTLD had three times as many registered domain names.²²

(b) Disputes

(i) In General

Over time, the registration and use of domain names has resulted in a variety of disputes, and their legal implications have been discussed thoroughly. The most important issues will be discussed below, as well as the methods applied in different countries and for different TLDs in respect to dispute resolution.

(ii) Cybersquatting

Cybersquatting is perhaps the most well-known reason for disputes over domain names. Cybersquatting can be defined as occurring when a person, the “Cybersquatter”, registers a domain name that rightfully “belongs” to someone else, e.g., someone registers a company’s registered trade mark, and the registration is made for the purpose of extorting the trade mark holder (in “bad faith”).

(iii) Reverse Domain Name Hijacking

Prior to the creation of ICANN and the UDRP, the gTLDs were provided by NSI,²³ and a policy was applied that allowed trade mark holders to place a domain name, identical with their registered trade mark, “on hold” pending resolution. The result of such an action, consequently, was that neither party could use the domain name.²⁴

The applied policy, however, did not take into consideration the fact that trade mark rights do not apply to non-commercial use. Reverse domain name hijacking can be defined as when a trade mark holder manipulates an implemented policy so as to take action in respect to domain names that would not have been possible solely based on trade mark rights.²⁵ Reverse domain name hijacking must, to some extent, have lost its importance, at least regarding the gTLDs, following the implementation of the UDRP and with it the condition that a domain name must be registered in “bad faith” to be transferred or cancelled (see text, below).

22 See www.dk-hostmaster.dk/dkhostcms/bs?pageid=101&action=cmsview&language=da.

23 This was achieved through a private corporation in contractual agreement with NSF and the United States government.

24 Jones, “Protecting Your ‘SportsEvent.com’: Athletic Organizations and the Uniform Domain Name Dispute Resolution Policy”, *West Virginia Journal of Law & Technology*, at <http://www.wvu.edu/~wvjolt/Arch/Jones/Jones.htm>.

25 Komaitis, “ICANN: Guilty as Charged?”, *Journal of Information, Law and Technology* 2003(1).

Yet, due to the far-ranging interpretations of the UDRP-regulations performed by some panellists, reverse domain name hi-jacking is still being discussed.²⁶

(iv) Misspellings

Misspelling is a form of cybersquatting that is done through the registration of a domain name similar to a popular domain name. As many people incorrectly spell or type the address in the web-browser, this registration is intended to capture traffic from the popular 'correct' domain name.

(v) Use of "Expired" Domain Names

Another method used to capture the traffic from a popular domain name is to renew its registration if the registration, intentionally or by mistake, has expired without being renewed. If the previous domain name holder does not have a trade mark right, there is almost no possibility of them recapturing the name.

(vi) Obscenities

In some cultures, the registration of words considered obscene is a large problem. The easy solution is to reserve words so that they cannot be registered. This might, however, be construed to be in conflict with the principle of freedom of speech; and it also must be understood that a word may have different, sometimes unfortunate, meanings in foreign cultures.

(vii) Defamation

Domain names can also be utilized in action opposed to a trade mark to express opinions regarding, for example, a company's behavior or policy. The most common example is the registration of ".sucks" domain names, i.e., a domain name constituting a company's name and the word "sucks" following it.

It has proven difficult to draw the line between cybersquatting and the freedom of expression, and panellists have interpreted the UDRP quite widely to close down ".sucks" sites. This has been criticized and has been considered contrary to the underlying purposes of the UDRP (see text, below).

(c) Dispute Resolution

As mentioned above, the "first to file" system is now the most common system for the issuance of domain names. Legal discussions regarding

²⁶ See the *Barcelona.com* case, where the domain name was transferred from a travel agency to the city of Barcelona with the motivation that the city had better rights. WIPO Case Number D2000-0505.

domain names therefore tend to mainly concern disputes, predominantly in relation to trade mark interests, and how they should be resolved, rather than discussions concerning which conditions should apply for registration.

Advantages of the “first to file” system include its speed and the fact that it makes the registration process simple; yet these very same factors can result in difficulties as the applicants are solely responsible for the control of a name prior to registration.

The “first to file” system can therefore enable the registration of a name that interferes with, for example, trade mark rights, and hence a condition for the system to function properly is that the applicants take responsibility when registering a domain name. As a result, the system can easily be used for illegitimate purposes, or two parties may both think that they are entitled to the same domain name. In both cases, there is a need for an effective forum that an aggrieved party can turn to for resolution of the dispute.

(i) Public Courts and Interpretation of Existing Legislation

One solution, used by several ccTLDs, is to allow public courts to interpret existing legislation and apply it to domain name disputes. The interpretation of trade mark law in relation to the regulations regarding freedom of speech has, in Germany for example, been considered to function adequately and to provide fair judgements.²⁷

Predictability in the rulings can be established through the use of precedents. The litigation process in public courts is, unfortunately, often too slow and costly to provide an effective solution.

(ii) New Legislation

A number of countries have considered domain name disputes as a basis with which to provide specific issues that need to be regulated by special legislation.

The most well-known example is the United States Anti-Cybersquatting Consumer Protection Act²⁸ that was created to prevent cybersquatting. The Anti-Cybersquatting Consumer Protection Act is applicable to registrations that are made in bad faith with the intent to profit from a protected trade mark (including a personal name) that is not registered to the applicant.

27 Papiri, “The Evolving System of Domain Name Dispute Resolution, section 99”, *Skifter utgivna av Institutet för Immaterialrätt och Marknadsrätt vid Stockholms Universitet*, number 115 (2002).

28 15 United States Code, section 1125(d).

(iii) Alternate Dispute Resolution Systems

To create an alternative to litigation in public courts, one that can resolve disputes quicker and less expensively, the majority of TLDs have chosen to implement special dispute resolution policies and alternative forums providing alternate dispute resolution systems (ADRs).

These ADRs are generally proceedings containing just one round of written pleadings that are made mandatory for all domain name registrants in the TLD. This is enforced by demanding that applicants for a domain name sign a contract ensuring that they must adhere to the ADR process.²⁹

The most important ADR is ICANN's Uniform Domain Name Dispute Resolution Policy (the UDRP) that applies to all of the gTLDs. The principles behind the UDRP were drafted by the World Intellectual Property Organization (WIPO) and implemented by ICANN in October 1999. The UDRP allows trade mark holders to seek arbitration against cybersquatters with the potential remedies of having the offending name cancelled or transferred. The UDRP was not supposed to replace the courts but instead to create globally uniform rules to be applied only to the most obvious cases of cybersquatting.

Compared to the previously applied NSI policy, the UDRP did not allow for the possibility of putting a trade mark on hold during the dispute resolution process; it also required that a domain name be registered or used in bad faith in order for a trade mark holder to initiate proceedings.

(d) Evaluation and Criticism*(i) In General*

The “.com” TLD is the most popular, and most of the discussion regarding the ADRs has thus far been focused on ICANN's dispute resolution system. This discussion has included important issues such as legitimacy, predictability, and freedom of speech, and has been too extensive to be thoroughly discussed here. A review of the various arguments and criticism follow below, with references to the most important decisions and work in the area.

(ii) Forum Shopping

The UDRP allows the complainant to choose from three different dispute resolution providers, the WIPO, the National Arbitration Forum (NAF), and the CPR Institute for Dispute Resolution (CPR). The UDRP has been criticized for enabling the complainant to choose the provider where it feels there

29 Geist, “Fair.com?: An Examination of the Allegations of Systematic Unfairness in the ICANN UDRP”, at <http://aix1.uottawa.ca/~geist/geistudrp.pdf>.

is the greatest possibility of winning by studying the statistics from previous decisions. A study performed by Professor Geist in 2001 showed that the WIPO handled 58 per cent of the total disputes and, in 82 per cent of the cases, it decided in favor of the complainant; the NAF handled 34 per cent of the disputes with almost 83 per cent of its decisions in favor of the complainant; while the CPR had only been engaged in 1 per cent of the cases, with the complainants winning 59 per cent of them.³⁰ The study has led to intense discussion and criticism of the UDRP. A simple solution that was applied by many of the ccTLDs who implemented their own ADRs instead of joining the UDRP has been to allow only one dispute resolution provider.

Another point reviewed in Geist's study, and closely related to forum shopping, was the possibility of choosing from either a single panellist or a three-member panellist proceeding. In disputes decided by a single panellist, the complainant has won 83 per cent of the cases while, in three-member panels, they have only won 60 per cent of the time. Both parties have the right to opt for a three-member panel, yet in consequence that party must then carry the cost for the two extra panellists. As a note of reference, 90 per cent of the UDRP-cases are decided by single-member panels.

(iii) Lack of Predictability

The UDRP also has been criticized for lacking predictability.³¹ The UDRP was initially supposed to be applied only to clear and obvious cases where a domain name was registered in "bad faith".

Many panellists have, however, applied the UDRP much more extensively and thus expanded the UDRP's area of application to cases that are more complex and demanding. The catalogue of behavior which constitutes bad faith is non-exclusive, and thus allows panellists to interpret it in a myriad of ways.

If the domain name has been registered for the purpose of "disrupting the business of a competitor", it is presumed to be registered in bad faith. In the decision *Dixons-online.com*, Mr. Abu Abdullah, a displeased consumer, was running a website that concerned a specific car dealer. It is noted in the UDRP decision that "there was no evidence to conclude the respondent is offering services or goods for any kind of commercial gain".³² Nevertheless Mr. Abdullah was considered to be a "competitor" and, thus, his domain name was registered in bad faith.

30 Geist, "Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP", section 2 (2001), at <http://aix1.uottawa.ca/~geist/geistudrp.pdf>.

31 Mueller, "Success by Default, A New Profile of Domain Name Trade mark Disputes under ICANN's UDRP", A Study Prepared for the Convergence Center, at pp. 22–25, at <http://dcc.syr.edu/markle/markle-report-final.pdf>.

32 ICANN UDRP Decision D 2001-0843.

The panel justified this by referring to a previous decision where it had been held “that competitor has a wider meaning and is not confined to those who are selling or providing competing products. In this wider context it means, one who acts in opposition to another and the context does not demand any restricted meaning such as commercial or business competitor”. This interpretation has been criticized for being unfair, contradictory to the legal and general definition of a “competitor”, and as being a threat to the freedom of speech.³³

Another example of the expansive interpretation of the UDRP has concerned the question of when a domain name is “identical or confusingly similar” to, e.g., a trade mark right, and thus can be transferred according to the UDRP. The most extensive interpretations and cases discussed involve a number of decisions regarding so-called “.sucks” domain names, e.g., websites with the primary purpose of expressing an opinion regarding a company or product and using a domain name which consists of said company’s trade mark or company name and, most typically, the word “sucks” thereafter.

Examples of decisions regarding such domain names are Guinnessreallysucks.com,³⁴ Wal-martsucks.com,³⁵ and Philpsucks.com.³⁶ All of these domain names were considered confusingly similar with the trade marks.³⁷

(iv) Lack of Legitimacy

Regardless of the form the system applied to control a TLD takes, voices have been raised in criticism of both the systems and their controlling organizations, in the international and the national TLDs. The dialogues and retorts have so far focused on legitimacy and citizens’ acceptance of the systems for the issuance of Domain names and dispute resolution. Legitimacy and acceptance can be obtained through many different methods, used not only by governments but also by the organizations controlling TLDs.

ICANN has been at the epicenter of these rebukes, with claims that it lacks legitimacy as well as acceptance. It has been argued that ICANN can rely on neither direct nor indirect public elections for legitimacy and that it also lacks the broad support of public opinion.

33 Mueller, “Success by Default, A New Profile of Domain Name Trade Mark Disputes under ICANN’s UDRP”, A Study Prepared for the Convergence Center, at pp. 22–25, at <http://dcc.syr.edu/markle/markle-report-final.pdf>.

34 ICANN UDRP Decision D2000-0996.

35 ICANN UDRP Decision D2000-0662.

36 ICANN UDRP Decision D2001-1195.

37 Other “.sucks” decisions include UDRP Decisions D2000-0584, D2000-0996, D2000-1015, D2000-0662, D2000-0477, D2001-0007, FA00102247, FA0097077, FA0097750, D2000-0636, D2001-1195, D2001-1195, D2001-0213, D2000-0681, D2000-0583, and D2000-1121.

As previously mentioned, the ICANN UDRP has been criticized for lacking independent panellists, and predictable regulations. In order for a system to be considered legitimate, the enforcement of powers must be clear and predictable and not give the impression of being arbitrary. Another shortcoming of the UDRP is its lack of a judicial review, as a judicial review would help bolster the commitment to process and rationality which becomes an important source for legitimacy.³⁸

(e) Differences between Countries

The manner in which a TLD is controlled has a large effect on its popularity and its functionality. First-to-file systems have proven much more popular than systems requiring a registered right to a name prior to registration. This is, of course, simply a consequence of the cost and trouble connected with registering a domain name.

Although some of the ccTLDs who impose requirements have satisfied their intention of preventing both cybersquatters and companies or individuals without a presence in their country from registering their domain names, they have failed to become the natural TLD for their countries. Due to the comprehensive regulations applicable on registrations in the Swedish TLD “.se”, for example, a majority of Swedish companies and individuals choose to register their name in the “.nu” TLD instead.

The Swedish TLD has now removed their requirements and are applying the First to file system. Another poignant example is the United States TLD “.us” that also previously applied rigorous requirements for the registration of its domain names, for example, registrations were only allowed under sub-domains that indicated the domicile of the registering company or individual. United States companies and citizens have chosen to primarily use the .com TLD instead of the United States TLD.³⁹

8.04 Other Issues

(a) Country Code Top-Level Domains

Although the “.com” TLD is still the largest TLD in terms of registered domain names, ccTLDs are increasing in importance. One good example is the German TLD “.de” that today has more than 8-million registered domain names and is rapidly and continuously increasing.⁴⁰ While the “.com” TLD

38 Weinberg “ICANN and the Problem of Legitimacy”, *Duke Law Journal*, volume 50, section 187, 2000.

39 See www.nic.us/faqs/index.html.

40 See <http://www.denic.de/de/domains/statistiken/index.html>, last visited March 2005.

was, just a few years ago, the only thinkable option for a commercial company, the ccTLD “.de” has now grown to become the number-one TLD for companies and organizations addressing the consumers and inhabitants of German-speaking countries.

This trend can be seen in ccTLDs all over the world, including smaller countries, but can of course be expected to have the largest impact in ccTLDs with large numbers of inhabitants. One example is the Chinese “.ch” that currently has only 430,000 registered domain names but is increasing steadily as Chinese inhabitants gain increased access to the Internet.⁴¹

The European Union (EU) announced its plan to introduce a new European ccTLD in 1999 but, due to the fact that the EU is not a “country” according to the ISO 3166-1 table, it could not be accepted as a ccTLD according to the ICANN ICP-1 policy document on country code delegations.

The EU Commission would not give up the idea of a European domicile on the Internet and, after extensive negotiations with the ICANN Board, the policy was changed. The ccTLD “.eu” is planned to be activated during 2005.⁴²

A ccTLD domain name enables the holder to address the population in one particular country directly in its own language and with a website attuned to the relevant market. Paradoxically, the most interesting effect that the ccTLDs might have is that the once-global Internet could become divided into different languages or geographic areas.

(b) Government Take-Overs

A direct effect of the ccTLD’s increased popularity is the growing interest from national governments. As a direct result of the universities’ strong influence in the beginning of Internet development, independent organizations were often assigned the responsibility of the ccTLDs.

In most instances, governments were not interested in the ccTLD as a national resource or considered it best administered by academic or non-profit organizations run by experienced enthusiasts. The Swedish ccTLD “.se”, for instance, was run for five years by a private citizen working at the Royal Institute of Technology. When the workload became too heavy, a non-profit organization was created to administer the TLD, draft rules for registration, and provide alternate dispute resolution.

41 15th Statistical Survey on the Internet Development in China (January, 2005), at <http://www.cnnic.net.cn/en/index/00/02/>.

42 Von Arx and Hagen, “Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control”, 9 *Rich. J.L. & Tech.* 4 (Fall 2002), at <http://www.law.richmond.edu/jolt/v9i1/article4.html>.

Many ccTLDs are today still controlled by academic or non-profit organizations, but national governments have begun to realize their importance and started to interfere. The governments of Switzerland, Australia, and Canada have seized full or partial control of their ccTLDs, while, in The Netherlands, a proposed bill would implicate an impending take over; and in Sweden the non-profit organization formerly in control of domain names has been forced, by the government, to change its rules for registration under the threat of a take over.

(c) “Generic” ccTLDs

Some ccTLDs have, primarily for economic reasons, chosen not to strive to become a national “zone” on the Internet, but instead to apply liberal rules for registration and to market their ccTLD towards other countries. In contrast to the government-controlled ccTLDs, which have a strong connection to a country’s inhabitants or to a particular language, is the corporate-controlled ccTLDs who address a global market, or even the inhabitants of a totally different country.

Possibly the most interesting example is that of the Tuvalu ccTLD “.tv”. Tuvalu is an island group in the South Pacific with a population of a bit more than 10,000. When Network Solutions first created the original ccTLDs, Tuvalu was abbreviated as “.tv”. The commercial potential of this ccTLD was quickly noticed by the corporation WebTV before the Tuvalu government was even aware of its existence. WebTV applied for and managed to be appointed as the representative of ccTLD. This would, however, not last for long, as soon the Tuvalu government gained knowledge of the situation and claimed the right to the ccTLD. The IANA then transferred the control of the ccTLD to the Tuvalu government, but the government was not interested in administrating the ccTLD and, instead, auctioned it to the highest bidder. Today, it is controlled by the “.tv corporation” and has no other relationship with the Tuvalu government than of paying royalties for its use of the TLD.⁴³

Other examples of ccTLDs which target markets other than their domestic market include the Niue “.nu” that is licensed to the United States corporation .NU Domain Ltd. and targets primarily the Nordic countries where “nu” translates as “now”; the Tonga “.to”, controlled by the private corporation Tonic with the Crown Prince of Tonga as the majority owner and targeting the global market, the Moldovian “.md”, controlled by the corporation Dot MD under a license from the government to issue domain names in English-speaking countries, primarily targeting medical doctors in the

43 See <http://www.tv/>.

United States; and the Samoan “.as”, controlled by the government but targeting the Norwegian market (where “as” translates as Inc.).⁴⁴

8.05 Conclusion

(a) In General

This chapter has dealt with the significant legal issues regarding the DNS. Several of these are of substantial importance, and jointly they are far too extensive to be discussed more thoroughly in this chapter.

One of the most interesting recent developments is the increasing importance of the ccTLDs. This also is the most pertinent issue in relation to the context of this chapter, and the discussion and conclusions will consequently focus on this issue.

(i) Increasing Importance of ccTLDs

The DNS, gTLDs, ICANN, and the connected dispute resolution system are all strongly influenced by western, particularly United States, interests. As a result of the United States advanced position in the development of information technology combined with its restrictive regulations for the issuance of domain names in the ccTLD “.us”, the gTLDs, and particularly “.com”, are dominated by United States companies and individuals.

Subsequently, as a reaction to this development, ccTLDs have gained in popularity, especially in countries where languages other than English are preferred in the contact with the domestic market and the citizens of the country; the fascinating popularity of the German “.de” is one example. Although many companies still operate from a central website divided into parts with different languages, generally registered in the “.com” TLD, it has become more common to also register the domain name in popular ccTLDs. This enables the domain name holder to address that country’s market directly from a national website.

This increased popularity of ccTLDs is likely to continue. Developing countries will rapidly increase their presence on the Internet as technological developments advance. Differences in culture and religion, as well as the recognition of languages and geographical areas as separate distinct markets that need to be independently addressed, will contribute to evolve. One excellent example that illustrates this point is the planned ccTLD “.eu”, whose issuance has been approved by ICANN following pressure from the EU.

44 “Location, Location, Location: The Geography of the Dot com Problem”, *Environment and Planning B: Planning and Design* 2001, volume 28, at pp. 59–71.

Accordingly, domain names in ccTLDs have become advantageous in the communication with citizens of different countries and distinct markets. From a legal viewpoint, this provides new perspectives on the previously discussed questions regarding the issuance of domain names and dispute resolution.

(b) Issuance of Domain Names in ccTLDs

The recent trend with reference to the issuance of domain names in diverse ccTLDs is a transition from systems requiring naming-rights for registration, into more liberal systems that apply the first-to-file principle.

This change is in reaction to the failure of the successful implementation of such systems. One difficulty with such systems is that they must compete with the gTLDs as well as other ccTLDs; applicants who are not allowed to register their desired domain name in one ccTLD may simply choose to register their name in another TLD. This has resulted not only in a loss of profits but, moreover, the ccTLDs' position as a natural zone for domain names related to that country is undermined.

The recent developments have now afforded new opportunities for ccTLDs to control which domain names are approved for registration. As the importance of a ccTLD increases, the alternatives become less attractive; for instance, when targeting the German market, a ".de" domain name has become almost a necessity. Although the requirements for name rights are not likely to be re-introduced, other techniques are being utilized to align ccTLDs with a country's national interests, e.g., cultural traditions, religious values, or desire for a national connection.

Such techniques are requirements for the applicant to be domiciled in the country and the reservation of names that are either not allowed to be used as domain names or reserved for the potential use of a certain party. Reserved names often include religious words, names associated with royal courts or states, and city or government authorities.

(c) Dispute Resolution in ccTLDs

Weighed against trade mark applications, the registration of a domain name is an uncomplicated, quick, and inexpensive procedure. Consequently, the increased importance of ccTLDs has caused international companies to 'vacuum' ccTLDs for salient domain names as a part of their trade mark strategy. The registered domain names might not only be trade marks held by the applicant company, but also generic words, abbreviations, and potential trade marks.

Another dissimilarity to trade mark applications is the fact that the DNS does not provide the possibility for dividing names into different classes of goods and services; furthermore, the DNS is an international system that addresses every geographical area in the world. While one name can be used as a trade mark in many different fields of goods and services and in many different countries or regions, that name converted into a domain name in a ccTLD is a scarce resource, creating potential conflicts between different trade mark holders. Coalesce this with ccTLDs becoming new markets for cybersquatters, and these disputes over competing legitimate interests result in the systems for dispute resolution taking on even greater importance.

Alternate dispute resolution methods have provided an alternative to traditional court processes that have proven effective enough to decrease cybersquatting in gTLDs. Although ADR techniques have been implemented in several ccTLDs, the situation is somewhat different. The costs for alternate dispute resolution procedures are often partially financed through the earnings of domain name registration fees in the TLD; this has resulted in fees for a complainant wishing to initiate a procedure that are reasonably low, often as low as US \$1,000.

In comparison to disputes over trade marks, this is very inexpensive but, conversely, there is rarely any possibility of transferring any of the cost to the opposing party, even if the decision is fully in favor of the complainant. If it is necessary to initiate procedures in several different ccTLDs, each having different rules for the resolution, costs both for the procedures and legal representation adds up to become quite substantial, and the administration become extensive.

The preferable solution would be a harmonization of all these many alternate dispute resolution methods, where a decision from any dispute resolution procedure would have a binding effect in all affiliated TLDs or a system where disputes would be resolved in one central alternate dispute organization, e.g., the ICANN UDRP. This concept is not a new one; the UDRP was created for the purpose of arbitrating not only disputes regarding domain names registered in gTLDs, but also in ccTLDs. WIPO published its ccTLD Best Practices for the Prevention and Resolution of Property Disputes back in 2001.⁴⁵ Despite the opportunity for ccTLDs to adopt the UDRP, a majority have instead opted to create their own ADR procedures; stating their motive as being the need to control the resolution of disputes related to their ccTLDs in accordance with differences in culture, religion, and differing views on trade marks, intellectual property rights, and freedom of speech.

45 See <http://arbiter.wipo.int/domains/ccTld/bestpractices/bestpractices.pdf>, last visited March 2005.

As a concluding remark, it should be mentioned that the future evolution of the DNS, and most especially the ccTLDs, is of exceptional interest as the activities of emerging economies, major languages, and developing countries influence the Internet. Concurrently, Europe is striving to delineate a part for themselves by demanding a new TLD of their own.

(d) Policy Issues

(i) In General

Finally, and taking into account the knowledge and conclusions discussed in this chapter, it is appropriate to provide a few comments and suggestions regarding the policy issues for the regulation of TLDs. These suggestions are of foremost interest to developing countries that have not yet dealt with the regulation of their ccTLDs.

(ii) Issuance of Domain Names

Distinct Interests The policy issues can be divided into two distinct areas, namely:

1. The regulation of the issuance of domain names; and
2. The dispute resolution of conflicts related to registered domain names.

The regulation of the issuance of domain names is dependent on which interests the policies aim to safeguard. The most fundamental interests to which a TLD may well give priority are:

1. Ensuring that registered names have a national connection;
2. Protecting trade marks;
3. Preventing disputes;
4. Ensuring that the right person has a particular domain name;
5. Profiting from registrations;
6. Ensuring usability and an uncomplicated registration process; and
7. Other specific interests, e.g., cultural or religious reasons for not allowing certain words to be registered.

Maximizing Profits It is easy to conclude that, if the main purpose is to maximize the profit of the TLD, a first-to-file system that is totally open for registration should be implemented.

This is the generally applied policy in the generic TLDs, as well as in national TLDs, such as the Niue “.nu” and the Tuvalu “.tv” that have successfully turned their fortunate delegation of ccTLDs into good incomes.

Rules for Registration If the policy aims to ensure that domain names have a national connection and to completely prevent disputes over trademark rights the solution is more complicated.

Systems with detailed rules for registration have, on the one hand, been proven to prevent disputes; on the other hand, they have been regarded as too bureaucratic and have caused applicants to choose alternative TLDs. These aspects need to be weighed against each other if the implementation of rules for registration are to be considered.

First-to-File System Based on present experience, including the fact that most policies with rules for registration have failed and have converted to first-to-file systems, the best suggested solution is for the TLD to apply a liberal policy and implement a first-to-file system.

Reserved words may be used to prevent culturally and religiously sensitive words from being used as domain names and to assure that certain names can only be registered by a specially entitled party, e.g., a local government or city. To serve the purpose of preventing trade mark disputes, trade marks can be reserved for the benefit of the trade mark holder. Reserved words should be published on the registrars' website in order to inform potential applicants and create trust in the system.

(iii) Dispute Resolution

Distinct Interests The policy issues related to domain name dispute resolution can in turn be divided into various areas where distinct interests may need to be safeguarded. Interests that need to be taken into account include:

1. Legitimacy;
2. Predictability;
3. Legal security;
4. Reasonably quick arbitration; and
5. Inexpensive arbitration.

Should a Policy Be Implemented? As a first step, it must be decided if an alternate dispute resolution policy and an alternate dispute resolution forum on the whole should be implemented or if disputes should be settled by public courts relying on existing or newly implemented legislation.

If the main objective is to safeguard the legitimacy, predictability and legal security of the system the dispute resolution may well be left to the public courts. In countries with established trade mark laws and experienced courts, this option has been proven to provide well-balanced and generally accepted decisions. Public courts do, however, have the severe disadvantage of being

very costly and relatively slow. At least for uncomplicated and relatively clear disputes, a quicker and cheaper alternative in the form of an alternate dispute resolution procedure is preferable.

(iv) Is Special Legislation Necessary?

The problem of solving disputes over domain names has existed in many countries for almost a decade. Some have chosen to implement special legislation, one example being the United States Anti-Cybersquatting Act, but others have instead relied on their general trade mark legislation and precedents. Both options have turned out well. Issues that cause difficult considerations and that can be solved through legislation include:

1. Creating a legal ground for the transfer of a domain name to the rightful owner (trade mark law generally only offers the possibility to impose prohibitions against use); and
2. Establishing the grounds for intervening against a domain name that has been registered in bad faith but which has not yet been used.

Decisions made by alternate dispute resolution procedures should preferably not be based on trade mark law but on a special, simpler, dispute resolution policy.

Adherence to the UDRP? If the TLD chooses to use alternate dispute resolution, it must decide whether to implement an existing policy, e.g., the ICANN UDRP, or to create its own policy. Developing countries implementing a new policy for dispute resolution can, with certain advantage, adhere to ICANN's UDRP.

Although the UDRP has been criticized, e.g., for lacking legitimacy and predictability, it has proven that it provides a practical working alternative for the resolution of trade mark disputes and is well known to domain name applicants on the global market. Consequently, despite its flaws, the UDRP will help provide trust in the TLD. Instead of attempting to create their own perfect systems, countries implementing alternate dispute resolution procedures should adhere to the UDRP and engage in the process of revising and improving it.

Arbitration Institute A TLD also must decide whether a new dispute resolution forum should be implemented or if one or all of the existing institutes for dispute resolution should be given the task. Based on the discussion related to arbitration, it can be concluded that the most important issue to address is the problem of forum shopping.

This problem can, however, easily be avoided by using only one arbitration institute. Whether one of ICANN's designated institutes is chosen or a

national institute is created is of less importance. Competent arbitrators can surely be found in either case. What is important is that every measure is taken to guaranty that the arbitrators are independent, in order to provide just decisions and legitimacy.

Transfer of Costs If the TLD has implemented an alternate dispute resolution procedure, the cost for the dispute resolution may be as low as US \$1,000, and many alternate dispute resolution procedures also reward the applicant with a reimbursement of half the cost if the claim is successful. The process generally consists of only one written statement, which helps to minimize the legal expenses and provide for a very inexpensive dispute resolution process as compared to a court process.

Despite these factors, the costs are not negligible and are definitely not for smaller companies and individuals; as a result, a market for “low-budget cybersquatting” can arise, i.e., cybersquatters demand an amount that is just under the cost for dispute resolution. In order to solve this problem, some TLDs, including the Dutch “.nl”, have implemented policies that allow the successful party to transfer legal expenses to the other party. This solution can be recommended, under the prerequisite that a relatively low limit for the allowed legal expenses is applied.