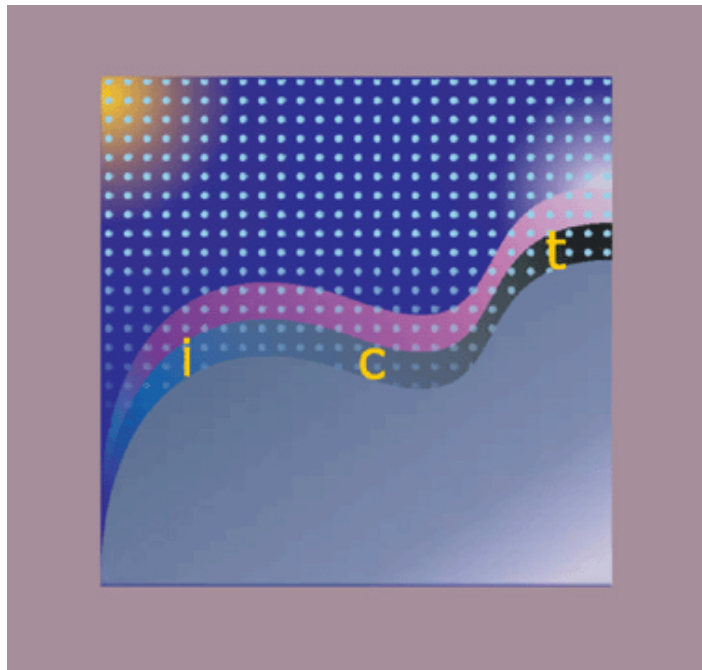


United Nations Conference on Trade and Development

E-COMMERCE AND DEVELOPMENT REPORT 2002

Internet version prepared by the UNCTAD secretariat



United Nations
New York and Geneva, 2002

Note

Symbols of United Nations documents are composed of capital letters with figures. Mention of such a symbol indicates a reference to a United Nations document.

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Material in this publication may be freely quoted or reprinted but acknowledgement is requested, together with a reference to the document number. A copy of the publication containing the quotation or reprint should be sent to the UNCTAD secretariat.

The Executive Summary of this Report can also be found on the Internet at the following address:

<http://www.unctad.org/ecommerce/>

UNCTAD/SDTE/ECB/2

Chapter 2

THE DOMAIN NAME SYSTEM AND ISSUES FOR DEVELOPING COUNTRIES

A. Introduction

The E-Commerce and Development Report 2001 provided a survey of key legal and regulatory issues arising with the development of e-commerce. As part of that broad review in chapter 6, the Report briefly addressed the issue of domain names,¹ providing in particular a jurisdictional analysis of the Anticyber-squatting Consumer Protection Act enacted in the United States in November 1999,² and considering also whether the domain name dispute resolution procedure adopted by the Internet Corporation for Assigned Names and Numbers (ICANN)³ – entitled the Uniform Domain Name Dispute Resolution Policy (UDRP)⁴ – provides a useful model more generally for alternative dispute resolution (ADR) or online (ODR) procedures.

This chapter seeks to provide more in-depth information concerning the development and functioning of the Domain Name System (DNS) and the use of domain names, while giving attention in particular to background, policies, initiatives and issues of relevance for developing countries. Even though the aim of this chapter is to provide a more thorough treatment, it cannot hope to cover all of the relevant information and issues of interest concerning domain names. Readers who wish to obtain additional information are referred to a number of useful resource sites on the Internet.⁵

The focus on domain names and the relevant concerns that have surrounded their emergence leads to a study of the various commercial, technical, regulatory and legal issues that have arisen more generally with the emergence of e-commerce and the increasing use of open communications networks such as the Internet. Unlike the telecommunications sector, which has historically been subject to international⁶ and State regulation of the large (often State-operated) tele-

phone system operators, the DNS has followed a very different path to development.

The rapid growth in use of the Internet has led to increasing importance being placed on the DNS as a secure and reliable general-purpose communications infrastructure. Yet the DNS, particularly in its earliest stages, has not been subject to centralized regulation through international treaty or otherwise, nor has its development been marked by the initiatives of large enterprises such as telecommunications operators.⁷ Instead, a key characteristic of the DNS, like the rest of the Internet, is that it functions through distributed computer networks largely under independent control, yet adhering to common technical protocols. Its rapid development has taken place at a time when self-regulation, rather than legislated international norms, is widely favoured in the “Internet space”. Moreover, a new generation of technology companies and Internet engineers, which have acted as a significant moving force behind the Internet’s development, have brought new perspectives and ideas to the policy discussions and debates on various issues. All of these elements together present a new and often confusing array of commercial, technical, legal and regulatory issues.

Developing countries attempting to build up their own national infrastructure to support increasing Internet use need to be aware of the multifaceted issues that may confront them. As many developing countries have already come to realize, the development of a national DNS infrastructure, including operative business model, technology and relevant domain name registration policies, could provide an incentive to citizens, local businesses and others to consider registering in the national top-level domain (e.g., such as “.br” for Brazil or “.th” for Thailand). This in turn would serve the goal of ultimately expanding online exchange of communications and information, and creating new channels for commerce.

B. Domain names: Coming into the mainstream

Domain names have evolved from an obscure technical detail of an experimental network into a well-known and widely used feature of the modern Information Society. As with a number of other typical e-commerce terms which would not have been commonly understood just 10 years ago, except perhaps among a small group of Internet engineers, the term “domain name” is now widely used in many countries and in different languages.⁸ Many people generally know what a domain name is and how it can be used. Use of the term, however, is not universal but reflects the same demographics as correspond more generally to the penetration of ICT and e-commerce worldwide.⁹

Hand in hand with this increasing recognition of domain names, registrations of the latter have grown at a rapid rate. As of the first quarter of 2002, just over 30 million domain names had been registered worldwide,¹⁰ compared with only 645 in July 1991 and 150,000 in late 1995.¹¹ The weekly volume of new registrations in 1999 was about 21,000,¹² and the number of domain name registrations overall is continuing to grow.¹³ This growth has recently been fuelled by the addition of new top-level domains (such as .biz or .info), discussed below.

1. Domain names and early Internet communication

(a) Defining a domain name

As background, we can review the specific meaning of the term “domain name”. Strictly speaking, an Internet domain is the name of a specific host that maintains a website and related sub-sites. A domain name consists of a string of alphanumeric ASCII characters, separated by periods, which is used to find a host on a network. For example, typing `www.unctad.org` into an Internet browser’s address box and pressing the return key will bring a user to the UNCTAD website. In addition, every host on the Internet has a unique address, which is a string of numbers called its “IP address”, just like a telephone number. The IP address, like the domain name, is usually expressed in dot notation, consisting of a numerical sequence that contains as many as 12 numbers in 4 blocks, separated by periods, e.g. `128.121.4.5`.¹⁴ Thus, each domain name can be mapped against a unique IP address. Domain names

were established because, with the increase in the number of Internet hosts, it became difficult to log on using long and difficult-to-remember IP addresses. The process of looking up the specific host’s IP address that corresponds to the entered domain name is called “name resolution”.

The infrastructure and technology used for name resolution is the Domain Name System. The DNS allows network users to easily locate and connect to host computers around the world. Technically speaking, the DNS can be described as a distributed, replicated, data query service chiefly used on the Internet for translating specific domain names into their underlying Internet Protocol (IP) numbers, which serve as the routing addresses for specific host computers located on the network.

Of course, domain names, as discussed below, have also taken on a second, overriding and non-technical function, serving as common business and personal identifiers.¹⁵ This function is much more in line with the widely held understanding of a domain name, particularly as its technical functions are, as with so many other user-friendly computer applications, invisible to the user. Thus, with the explosion of interest in the Internet following the advent of the World Wide Web domain names have come to be considered a valuable part of many companies’ brands.

Domain names can be expected to continue to play an important role in business and for other non-commercial, public or personal purposes. This is particularly true since a domain name effectively serves, at one and the same time, as a branding or identification device for a business, an organization or a person, and as the functional mechanism to locate its website. The domain name has thus evolved to present a novel and potent characteristic by combining these two features into one user-friendly label. As the use of ICT and e-commerce spreads in developing countries, these same powerful features should serve to give domain names equal relevance for both commercial and non-commercial uses in those countries. As discussed below, policy decisions are required in relation to the national country code top-level domains (ccTLDs) in order to foster not only ease of registration of domain names but also overall confidence in the relevant ccTLD space so that domain names can be as useful as possible.

(b) The Internet's early development¹⁶

The early users of the Internet consisted largely of a group of volunteers and academics, some of whom received funding from the United States Government. These pioneers experimented with establishing communications between the computers connected to their networks. In 1969, when the Internet's predecessor, the Advanced Research Projects Agency Network (ARPANet), was established, it consisted of just four host computers connected to the network. It was small enough that the users generally knew how to locate and communicate with each other; identification of the network's computers did not cause difficulties.

Dr. Jon Postel, a computer scientist at the University of Southern California's Information Sciences Institute (ISI), is regarded as a pivotal figure in the development of the Internet's address system. For many years, he played a central role in the technical management and administration of the Internet, acting as director of the Internet Assigned Numbers Authority (IANA), again a United States financed entity. He was one of the small group of computer scientists who created the ARPANet, and worked on the development of early Internet protocols and standards.¹⁷ The Request for Comments (RFC) 1591, authored by Dr. Postel in March 1994, addresses the "Domain Name System Structure and Delegation" and is regarded as having set out the basic principles for the DNS. Dr. Postel's early stewardship of the Internet address system is credited with providing the foundations to enable the fast-growing high-speed international communication network to eventually connect computers throughout the world.

In 1974, a further key technical advance was the development of a new host-to-host-protocol, introduced by two other Internet engineers, Bob Kahn and Vint Cerf, called the Transmission Control Protocol (TCP). It was designed to meet the needs of an "open" architecture network (as compared with a closed, private computer network) and eventually, in 1978, it was broken into two parts, TCP, which was charged with breaking up and reassembling the data messages sent across networks, and IP (Internet Protocol), which was charged with the routing of the data. The standard, now central to Internet communications, thus became known as TCP/IP.

Next in the development of the DNS, in 1983, another engineer, Paul Mockapetris of ISI, created a naming system which mapped IP addresses to easily remem-

bered names. Each computer was allocated to a unique domain name and the computer's IP address would be converted into this name, and vice versa. When the user typed in the name, it would be automatically changed to the appropriate IP address and the corresponding computer on the network could be located. Furthermore, under the new system, no single machine maintained information on all the host machine names. Instead, each administrator maintained the information on its own hosts, and a central authority kept records on the location of this information, thus establishing the distributed nature of the system.

The Domain Name System had been created.

Following these formative developments, Network Solutions Inc. (NSI), a privately owned company located in Virginia in the United States, was contractually given the right by the United States Department of Commerce to register domain names on behalf of the public.¹⁸ In 1995, NSI was allowed to begin to charge a fee for DNS registrations. NSI registered domain names in what are known as the generic Top Level Domains (gTLDs) on a first-come-first-served basis. The first seven of these gTLDs, established in 1984, are well known: .com, .org, .net, .gov, .edu, .mil and .int.

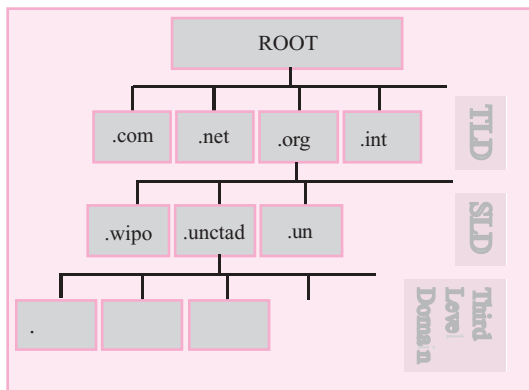
In response to a United States Department of Commerce White Paper published in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was created the same year. Regarding the management of the DNS, ICANN's core mission is to continue the work of IANA, although in a more formalized and globally representative framework in order, in its own words, "to ensure the views of all the Internet's stakeholders are taken into account in carrying out this public trust".¹⁹ In consequence, ICANN assumes responsibility for overseeing the technical coordination of the DNS. As part of this function, it approved the introduction of seven new gTLDs in November 2000, namely .aero, .biz, .coop, .info, .museum, .name and .pro.

As domain names have become increasingly important for a variety of uses, new legal issues have presented themselves, the most important of which is the potential conflict between domain name registrations and trademark rights. This issue is addressed fully below, and represents a significant recent chapter in the history of the DNS.

An obvious yet important aspect of this brief DNS history, relevant even today as discussions continue

through ICANN on how to implement an international structure for oversight of the DNS, is that much of the early critical planning and work took place in the United States, sometimes with government assistance. This United States influence continues to be strong, as reflected for example in the geographical placement within the United States of most of the strategic DNS “nameservers”, which are important to the overall functioning of the DNS (see below). While the United States Government has facilitated efforts to secure more international participation and input into decisions concerning the DNS, developing countries should be encouraged to become more involved so that their concerns and requirements in relation to the DNS can be heard and advanced.

Chart 3
Authority concept of the DNS



(c) Functioning of the DNS

When the DNS was introduced, an extremely important concept was the dividing of the single list (managed by ISI) into hierarchical layers or “domains”, thus introducing at one and the same time the concepts of authority and decentralized functioning. Under this system, higher-level domains have authority over the sub-domains beneath them. For example, in the (fictional) domain of `www.ecommerce.unctad.org`, the `.unctad` domain would have authority over `.ecommerce`. This domain concept can be expressed by means of an inverted tree diagram, in which everything is subordinate to the “Root” (see chart 3) and each sub-domain is subordinate to the domain above it. Keeping in mind the authority concept, domain names are read from right to left. In the example of `www.ecommerce.unctad.org`, the `.org` constitutes the so-called top-level domain (TLD); `.unctad` is called the second-level domain (SLD); and `.ecom-`

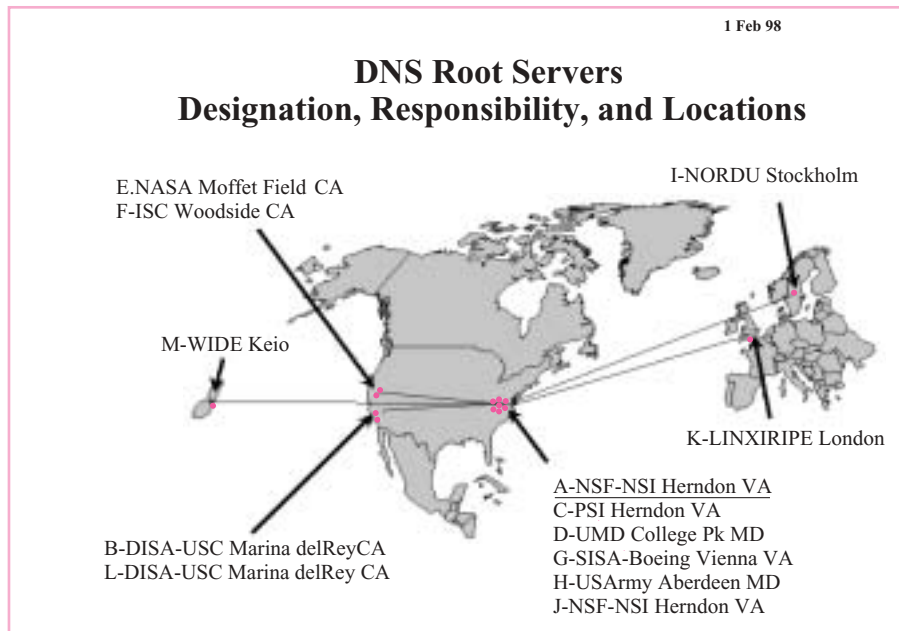
merce constitutes the third-level domain. This designation of levels is the same irrespective of the level’s content. Thus, the SLD can represent the name of the business, organization, individual or something else. Rules applicable to the higher-level domain are usually to be incorporated into the next sub-level, along with any rules which that sub-level may introduce.²⁰ This allows for the decentralized (by sub-domain) administration of the DNS. Practically, this has permitted the creation of a private system of management for the DNS, in which obligations can be imposed by contract from one domain level to the sub-domain.

From a technical perspective, at the heart of this DNS system are 13 special computers, called root servers, which are the ultimate technical infrastructure of the DNS and are of major importance for the functioning of the Internet. They are coordinated by ICANN and are distributed around the world, with ten located in the United States, two in Europe and one in Japan (see chart 4). All 13 contain the same vital information – this is to spread the workload and back each other up. The root servers contain the IP addresses of all the TLD registries – both the global registries such as `.com` or `.org`, and the country-specific registries such as `.fr` (France) or `.cn` (China). This is critical information; if it is not 100 per cent accurate or if it is ambiguous, it might not be possible to locate a website on the Internet.

The “A” root server constitutes the most important authority of the system. It is operated by Verisign. This A-Server contains the authoritative copy, stating which nameservers hold the relevant information for each of the top-level domains. The authoritative copy is the one that all other root servers trust to be authentic and contains the most complete and most updated list (the so-called zone file) of the TLDs. This is why the other root servers, which are operated by several independent organizations,²¹ direct their requests to, and copy their information from, the A-Server.²²

This technical structure shows that the DNS, while working with a decentralized infrastructure and administration, is nevertheless based on a root server system which has a centralized and authoritative hierarchy. The system has been designed to ensure predictable look-up results from anywhere on the Internet, a concept known as “universal resolvability”. It is a critical design element of the DNS. This is similar to the telephone system: when a telephone number is dialled, it rings at a particular location because there is a central numbering plan ensuring that each telephone number is unique. If telephone numbers or domain names

Chart 4
Authoritative root server system



were not globally unique, phone calls or e-mail intended for one person might go to another. Without uniqueness, both systems would be unpredictable and therefore unreliable.²³

In this context, it is worth noting that some private companies have recently introduced new gTLDs which can be accessed by “alternative roots”. They are not tied into the single A-root hierarchy discussed above, although some operators claim they are being unfairly excluded. Problems can be caused by these alternative roots, including lack of reliability. Those purchasing domain names in these pseudo-TLDs may not be aware of the consequences arising from lack of universal resolvability. As noted above, if the DNS must make a choice between two identical domain names with different IP addresses (i.e. one in the A-root system and one registered under an alternative root), the DNS would not function properly. These problems are insignificant so long as the alternate roots remain very small; however, if they should ever attract many users, the problems would become much more serious, and could affect the stability and reliability of the DNS.²⁴

Authorities in developing countries should be aware of the architecture and functioning of the DNS, so that they can make appropriate choices in relation to international policy, as well as implementation of national policy. Each country should be concerned about

establishing a reliable DNS environment, so that predictable look-up results can be achieved by entering a domain name, just as dialling a telephone number should permit completely reliable contact. Adhering to universal resolvability will promote confidence in online communications, allowing countries to take full advantage of the Internet as a resource for information, education and commerce.

More information explaining the operation of the DNS is provided in annex A.

2. Top-level domains TLDs : Generic and country code TLDs, and new multilingual variations

As noted, the DNS operates on the basis of a hierarchy. Although there is no difference functionally, the top layer consisting of TLDs is divided into two categories: generic TLDs (gTLDs) and country code TLDs (ccTLDs). Both gTLDs and ccTLDs are an integral part of the Internet infrastructure, promoting global interoperability in the DNS.

(a) gTLDs

The gTLDs are top-level domains which are not associated with any country, territory or geographical area. Therefore, policy and planning decisions regarding

their operations generally do not fall within the purview of a particular Government, but are left to the particular sponsoring organization or registry operator, acting under the auspices of ICANN.²⁵ As noted above, initially there were seven gTLDs, three of which are “open” or unrestricted (.com, .net, .org) and the other four of which are restricted (.edu, .gov, .mil and .int). In November 2000, seven additional gTLDs were introduced by ICANN, notably, .aero, .coop, .biz, .info, .museum, .name, and .pro. Thus far, five of the new gTLDs are operative and accepting domain name registrations.²⁶

The gTLDs commonly use extensions to denote the purpose intended for the TLD. The .com TLD is intended for commercial entities, .edu is reserved for educational purposes, .net is for computers of network providers and .org is for charity or non-profit organizations. However, today, only the .int (international organizations), .gov (United States Government) and .mil (United States military) domains follow strictly their original restricted policies for registration. As for the others, the limitations have never been enforced and their categories have become blurred with time. The .com TLD, favoured by many as the domain name registry of choice because of its wide name recognition, has evolved into a catch-all premium registry.

The newly introduced gTLDs also follow registration policies based on function and are intended to be limited to certain groups of individuals, companies or organizations.²⁷ The .biz domain is reserved for business or commercial purposes, whereas .name is limited to use by individuals. Registration for the .pro TLD will be limited to professionals – accountants, lawyers and physicians. The .aero, .coop and .museum TLDs are reserved for the air transport industry, cooperatives and museums, respectively. The only new gTLD that is intended to be used in a completely unrestricted manner is .info. However, only the future will show whether the registration limitations of the other TLDs are in fact applied rigorously. In this context, it is interesting to note that the registry operator for the new ICANN-accredited .biz TLD has implemented a Restrictions Dispute-Resolution Policy (RDRP), under which any third party may file a complaint about the registration or use of a domain name which is in violation of the domain name registration restrictions.²⁸

Table 10 sets out the gTLD, sponsoring organization and restrictions, if any, applicable to the 14 gTLDs.

The seven new gTLDs were introduced in order to expand the generic name space available for registra-

Table 10
Sponsored gTLD agreements

gTLD	Open/restricted	Sponsor
.aero	Reserved for members of the air transport industry	Société Internationale de Télécommunications Aéronautiques (SITA)
.biz	Restricted to businesses	NeuLevel, Inc.
.com	Open	VeriSign Global Registry Services
.coop	Reserved for cooperative associations	Dot Cooperation LLC
.edu	Reserved for degree-granting educational institutions of higher education	Educause
.gov	Reserved for the United States Government	US General Services Administration
.info	Open	Afilias Limited
.int	Reserved for organizations established by international treaties between Governments	IANA .int Domain Registry
.mil	Reserved for the United States military	US DoD Network Information Center
.museum	Reserved for museums	Museum Domain Management Association
.name	Reserved for individuals	Global Name Registry
.net	Open	VeriSign Global Registry Services
.org	Open	VeriSign Global Registry Services
.pro	Reserved for certified professionals	RegistryPro, Ltd

tion of new domain names, and to promote competition in gTLD registration activities. While .info or .biz may be considered similar in design to the existing open gTLDs (i.e. .com, .net and .org), the others such as .aero, .coop and .museum introduce a new element of differentiation, which can serve as an instrument for sending signals to the Internet user while advancing the policy objectives of these registries.

As new gTLDs are introduced, developing countries have an opportunity to take advantage of the new name space becoming available, although certain commentators have suggested that many of the useful names in the .com TLD have already been registered. Groups in developing countries may also, in the future, wish to sponsor new gTLDs that would support their own objectives, in view of the market-signaling power that a TLD can exhibit.²⁹ Of course, the ccTLD space, discussed below, is the natural starting point for serving the national goals and policies of each country. Furthermore, the new space and dimensions that will be brought into being by enabling the registration of multilingual domain names (discussed below), which reflect the linguistic diversity of Internet users, mean that the potential resource space for domain names, even in the existing gTLDs, is greater than many may have previously believed.

(b) Country code top-level domains

Country code TLDs (ccTLDs) are two-letter domains – such as .ag (Antigua and Barbuda), .lk (Sri Lanka), .pa (Panama) and .sn (Senegal) – which correspond to a country, territory or other geographical location. They bear two-letter codes based on the official list maintained by the International Organization for Standardization (ISO) in its International Standard 3166. In that connection, ICANN, in its role of coordinator of the delegation of codes for ccTLDs, issued a resolution in September 2000 reaffirming that

“alpha-2 codes are delegable as ccTLDs only in cases where the ISO 3166 Maintenance Agency, on its exceptional reservation list, has issued a reservation of the code that covers any application of ISO 3166-1 that needs a coded representation in the name of the country, territory or area involved.”³⁰

Currently, there are 243 ccTLDs.

The rules and policies for registering domain names in the ccTLDs vary significantly. Although these domains were originally envisioned as being limited to domestic use,³¹ the registration policies of various

ccTLDs have evolved differently. The registry for each ccTLD sets its own policies for domain name registration. Some ccTLDs are reserved for use by citizens or local entities within a particular country,³² while others are operated in an open and completely unrestricted manner. In fact, there are approximately 80 open ccTLD registries, in which any organization or person can register a name generally on a first-come-first-served basis. Thus, for example, domain names can be registered by anyone in the .to, .tm or .as. ccTLDs, corresponding to Tonga, Turkmenistan and American Samoa respectively.

Generally speaking, the ccTLD registries are operated by local administrators in each country. Initially, these administrators were usually drawn from technically skilled personnel, sometimes associated with an academic institution. Today, the administrators of ccTLDs come from the private sector or educational institutions, while others are under governmental control.

It is not uncommon that for certain ccTLDs the local administrator has introduced functional categories similar to those available in the gTLDs, but residing at the level of the second-level domain (SLD) in the DNS. The registration of a domain name by an interested person, therefore, takes place at the third-level domain. For example, the registry for the United Kingdom's .uk ccTLD space,³³ Nominet.UK, has implemented the following SLDs in which domain names can be registered by users:

- *ac.uk* (reserved for academic institutions, e.g. *www.oxford.ac.uk* for Oxford University);
- *ca.uk* (reserved for commercial enterprises – the largest SLD under *.uk*);
- *.gov.uk* (reserved for the United Kingdom Government);
- *me.uk* (open to individuals);
- *org.uk* (open to non-commercial organizations);
- *net.uk* (reserved for Internet service providers);
- *ltd.uk* and *plc.uk* (reserved for registered company names only);
- *sch.uk* (reserved for schools).

In Sweden, as another national ccTLD example, certain periodical publications can be registered under the

press.se SLD, while private individuals can register a domain name under the pp.se SLD.³⁴

Early on, any agreement between the ccTLD operators and IANA (as the organization providing technical oversight of the DNS) to implement coordinated policies for the Internet was informal at best. In many instances, although IANA had introduced a designated two-letter country code into the A-root, there were continuing disagreements about who should be the authorized administrator of a particular ccTLD.³⁵ As the Internet has spread and grown in commercial importance, many commentators, businesses, Governments and users of the Internet have concluded that a more formal set of agreements should be established.

One of ICANN's principal activities thus has been to work with the other organizations involved in the Internet's technical coordination to formally document their role within the ICANN process and their (and ICANN's) commitments to implement the policies that result. This focus has resulted in agreements between ICANN and a number of different DNS players, including VeriSign, formerly Network Solutions, which operates the .com, .net and .org TLDs; the companies responsible for operating the new 'unsponsored' TLDs (.biz, .info and .name); the organizations establishing the 'sponsored' TLDs (.aero, .coop and .museum); over 150 ICANN-accredited registrars; the regional Internet registries; and the Internet Engineering Task Force.

Since 2000, ICANN has also been working with managers of ccTLDs to formalize and document their relationship with it. These relationships can be more complex, because of the varying circumstances (in terms of type of organization, policies, language, culture, legal environment and relations with Governments) of different ccTLDs and the organizations that operate them. The ICANN Government Advisory Committee (GAC), an ICANN advisory body composed of representatives of Governments, has been instrumental in this area. Through several communiqués provided to the ICANN Board of Directors, the GAC has established the following positions:

- The Internet naming system is a public resource and the management of a TLD Registry should be in the public interest.
- Accordingly, no private intellectual or other property rights should inhere in the TLD itself

or accrue to the delegated manager of the TLD as the result of such delegation.

- The delegation of a ccTLD Registry (to a particular operator/manager) is subject to the ultimate authority of the relevant public authority or Government.

These positions were formalized in a GAC document entitled "Principles for Delegation and Administration of Country Code Top Level Domains", which was published in February 2000. This document provides, in the relevant part, that:

"The delegee of a ccTLD is a trustee for the delegated domain, and has a duty to serve the residents of the relevant country or territory in the context of ISO 3166-1, as well as the global Internet community. . . Its policy role should be distinguished from the management, administration and marketing of the ccTLD. These functions may be performed by the same or different entities. However the delegation itself cannot be sub-contracted, sub-licensed or otherwise traded without the agreement of the relevant government or public authority and ICANN."

ICANN recently introduced a "Model ccTLD Sponsorship Agreement", which aims at regulating the rights and obligations between ICANN and ccTLD administrators, and also defines the role of the governmental authority in the ccTLD environment.³⁶ For ICANN's part, the Sponsorship Agreement provides that ICANN will maintain a stable, secure and authoritative database of relevant information about ccTLDs maintained in the "Authoritative Root-Server System". Thus, for a particular ccTLD, the Authoritative-Root Database will contain all relevant information to ensure its proper technical functioning, including information about the ccTLD sponsoring organization (with administrative and technical contacts) and certain other technical information (i.e. regarding the ccTLD nameservers). The ccTLD sponsoring organization, on the other hand, agrees to use its best efforts to operate the ccTLD in a stable and secure manner, so that domain names registered within the ccTLD are reliably resolved for users throughout the Internet. As regards the relevant governmental authority, the Sponsorship Agreement mainly emphasizes its responsibility for the public interest on behalf of the Internet community in the country in question, and coordinating in relation to the ccTLD administrator's management of the ccTLD.³⁷

Importantly, the Sponsorship Agreement would also require ccTLDs to make a financial contribution to ICANN's cost of operations. For example, an appendix to the Agreement provides that for the year ending 30 June 2002, the maximum fixed annual contribution is \$5,000, with this amount set to automatically increase by 15 per-cent on 1 July of each year.³⁸ It may be increased by a greater amount if new or revised ICANN policies are established. The appendix further provides that the total amount of fees paid by all TLD sponsors and registry operators that have sponsorship agreements with ICANN cannot exceed the annual cap of \$5,500,000, but this annual cap will also increase by 15 per-cent each year. For developing countries, particularly with ccTLD registries in which there are very few domain name registrations, these fee obligations to ICANN can represent a significant financial burden.

Aside from the ICANN Sponsorship Agreement, other issues for ccTLDs concern the environment for competition in respect of domain name registry and registrar services. These services may be structured quite differently, depending on the particular policies in the country concerned. Registry services relate to organizing, managing and administering the ccTLD name space – including the central authoritative database for the ccTLD and associated public query services – in a secure and reliable manner. Registrar services, on the other hand, are directed towards interacting with customers, offering these “registrants” services for registering their domain names in the ccTLD.

In Germany, for example, the administrator of the .de ccTLD³⁹ in addition to being the operator of the registry, offers services as a domain name registrar. However, the administrator actually recommends that users register their domain names with other registrars and only offers its registration services at a price which is less competitive than the prices offered by other registrars in Germany. Some ccTLD administrators act as both the sole registry and registrar for the relevant country domain space, especially in those countries where domain names have not yet proved to be so popular. Still other ccTLD administrators, as in Germany, have announced their intention of introducing a more competitive environment for domain name registration activities within their ccTLD. This is the case for the government-owned Singapore Network Information Centre (SGNIC), administering the .sg ccTLD. Currently, SGNIC maintains the registry for .sg and is also the only organization acting as registrar to accept domain names registrations in this ccTLD. Soon, how-

ever, other companies will be invited to become accredited registrars, thus competing at the registrar level for domain registration business in Singapore. SGNIC will, however, maintain control of the registry.⁴⁰

Given the technical requirements, it is widely accepted that it would be extremely difficult, and would put DNS reliability at risk, to introduce competition at the level of registry services for a particular TLD. Thus, two different entities should not share registry services for a given TLD. However, competition among registrars is now common. As noted above, there are more than 150 ICANN-accredited registrars competing around the globe to accept domain name registrations and offer related services in the gTLDs. Further information about the market for domain name registration services is provided in section B.3 below.

In developing countries, ccTLD administrators can develop appropriate policies that meet the needs of their community, satisfying any relevant legal, cultural, economic, language or other requirements. There is no single model for structuring a ccTLD that would fit the needs of all countries or territories. The policies for each ccTLD should be carefully formulated with all of these particularized factors in mind, with the overall goal of promoting access to and use of the Internet. In order to illustrate the different registration policies that may be implemented by different ccTLDs operators, the policies developed for the Republic of the Congo (.cg) are briefly highlighted in box 1.

As a further example of new developments in this area, the European Union on 30 April 2002 published a new Regulation to “implement the .eu country code Top Level Domain (ccTLD) within the Community”.⁴¹ The .eu ccTLD was first proposed as part of the EU's e-Europe initiative to accelerate the development of electronic commerce.⁴² The EU believes that the new .eu ccTLD will “accelerate the benefits of the information society in Europe as a whole”, and, in particular, provide greater visibility for the EU Internal Market on global information networks, while increasing choice and competition.⁴³ Furthermore, it is viewed as a positive factor that the infrastructure accompanying the implementation of the .eu ccTLD, including DNS nameservers and the registry database for .eu, will be located in the EU and will therefore “affect the topology and technical infrastructure of the Internet in Europe”.⁴⁴ It is envisaged that the European Commission will establish a fair selection procedure to designate the entity that will act as the registry for .eu. The Regulation also specifies that the

Box 1

Republic of the Congo (.cg) ccTLD

The administrator for the .cg ccTLD is the Network Information Center (NIC) of the Republic of the Congo. It has posted its registration policies on the web at www.nic.cg. The .cgNIC serves both as the registry and the registrar for domain names registered in this space. It has established the following policies:

- Registration is free of charge for the citizens or lawful residents of Congo (may require copy of passport or residence permit to be produced).
- A company or non-governmental organization registered and operating in the country will also qualify for free domain name registration services.
- Legal institutions, government ministries, churches and other authorities of Congo have the highest priority with regard to the right to free domains.
- Foreign entities are not precluded from registering in the .cg ccTLD; however, these entities are charged a registration fee. The fee is currently 550 Swiss francs for the first year, and 350 Swiss francs for each year thereafter.
- While domain names may be registered directly in the SLD under .cg (e.g. unctad.cg), the domain name must have a minimum of three characters. Two-letter domain names may be registered only with special authorization.
- The – *gov, net, edu, ac, com, co, int, mil* - sub-domains are considered restricted.
- The use of the misleading suffix .cg is strongly discouraged: users are reminded that .CG stands for the Republic of the Congo and for nothing else.

registry will operate on a non-profit basis and will not itself act as a registrar. The .eu initiative is a relevant example for developing countries of how a ccTLD can be implemented, even on a regional basis, to broadly promote the objectives of increased Internet usage and e-commerce activity, as well as regional recognition and integration.

Additional resources for operating a ccTLD registry are becoming more widely available for the managers of ccTLDs. Developing countries can take full advantage of these materials as they determine their own policies. For example, the ccTLD Constituency of ICANN, a group representing ccTLD administrators in the ICANN process, has produced “Best Practice Guidelines for ccTLD Managers”.⁴⁵ The Guidelines provide that (a) ccTLD registries should ensure that there are standard agreements for domain name registrants setting out the expectations and obligations of each party; (b) ccTLD Managers should be fair to all eligible registrants requesting domain names; (c) policies and procedures may vary from country to country owing to local customs, cultural values, local policies, law and regulations; (d) the policies and procedures for the use of the ccTLD should be made available for public inspection; (e) ccTLD Managers should have a policy on privacy and that policy should be published;

and (f) ccTLD Managers should define and publish their domain name dispute resolution policies and procedures in consultation with the Local Internet Community (making judgements in relation to disputes between third parties and domain name registrants is outside the scope of the ccTLD Manager’s duties).

The World Intellectual Property Organization (WIPO) has also published a useful guide, the “WIPO ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes”.⁴⁶ This statement of best practices is intended to establish a set of minimum standards for the protection of intellectual property in the ccTLDs, particularly in respect of open ccTLDs (i.e. ccTLDs in which there are no restrictions on the persons or entities registering). The WIPO Best Practices focus on three elements:

- *Registration agreement*: a prerequisite for the proper management of a ccTLD is that the rights and obligations of the domain name registrant and the ccTLD administrator should be reflected in a formal registration agreement.
- *Contact details*: the collection and making available of domain name registrant contact details is

important for facilitating informal steps or initiating formal procedures aimed at redressing intellectual property infringements.

- *ADR*: ADR procedures for resolving disputes between domain name registrants and trademark owners can provide an efficient, fair and inexpensive approach.

WIPO has also established a comprehensive “WIPO Ecommerce ccTLD Database”, which contains links to 243 ccTLDs and provides information about their registration agreements, WHOIS services and alternative dispute resolution procedures.⁴⁷

One further development of significance to ccTLDs is the formation of regional ccTLD groups, which have developed over the last several years as a resource for ccTLD managers and to more effectively voice concerns that regional ccTLDs operators may have. Developing countries may find that the information and contacts available to them through these organizations will be extremely helpful. A number of them also participate actively in the ICANN process.

The African Top Level Domains (AFTLD) project, for example, was established for ccTLD registries in

Africa and the Middle East to cooperate and engage in concerted action on issues of common concern. The AFTLD website provides further information.⁴⁸ AFTLD lists its objectives as follows:

- Representing the interests of the African ccTLDs, including the neighbouring islands around the African continent;
- Promoting communication and cooperation between ccTLDs’ managers;
- Informing the African Internet community about the ICANN process through an awareness and outreach programme; and
- Providing a common address where information about African ccTLDs can be obtained.

Box 2 provides information about relevant ccTLD organizations and forums.

These resources, as well as others, show that an increasing amount of information is becoming available to developing country experts to assist in the formulation of an appropriate approach for management of a country domain space. Information concerning registration policies, as well as model implementation agreements, can also be found online, through the ICANN website.⁴⁹

Box 2

TLD forums

- | | |
|--|--|
| • African Top Level Domains (AFTLD) | www.aftld.org |
| • AfriDNS | www.afriDNS.org |
| • Asia Pacific Top Level Domain Forum (APTLD) | www.apTld.org |
| • Latin American & Caribbean Country Code Top Level Domain Organization (LACTLD) | www.lactld.org |
| • North American Top Level Domain Organization (NATLD) | www.natld.org |
| • Council of European National Top-Level Domain Registries (CENTR) | www.centR.org |
| • International Association of Top Level Domains | www.iatld.org |
| • World Wide Alliance of Top Level Domain-names | www.tld.org |

(c) Multilingual (“internationalized”) domain names

A new development, which stands side by side in importance with the expansion of the gTLD space and

the continuing development of ccTLDs, is the emergence of multilingual or “internationalized domain name” (IDN) technology. This refers to DNS technology that will allow Internet users – for example, those whose native language is not English⁵⁰ – to use lan-

guage character sets other than the Latin (also described as Roman) ASCII set,⁵¹ which is today the only set (including letters, numerals and hyphens) that can be used for domain names. Thus, with the implementation of IDN technology, domain names will be able to be expressed, for instance, in Arabic characters.⁵² There are several commercial initiatives under way to make domain names available in character sets other than the Latin ASCII.⁵³ Meanwhile, a key standards-setting body for the Internet, the Internet Engineering Task Force (IETF), is actively discussing the appropriate technology and protocols which should be adopted as a standard in this area.⁵⁴

These new developments have an obvious relevance for developing countries. There is broad recognition that IDNs offer the potential to increase Internet use for a significant segment of the world's population, whose native language is written in non-Latin scripts. For example, a person in China, rather than searching for a term in the English language (using the Latin ASCII script) to express an identity, brand or concept in a domain name, can use the IDN technology to choose a domain name in a Chinese character script. When implemented, the IDN technology will make possible the natural logic of allowing one to express oneself in one's own language, while also bringing new registration space to the DNS.

These IDN developments have been followed closely by ICANN. It has established an Internationalized Domain Names (IDN) Committee. The ICANN Board of Directors, in a resolution dated 25 September 2000, recognized "that it is important that the Internet evolve to be more accessible to those who do not use the ASCII character set". The resolution emphasized, however, that

"the internationalization of the Internet's domain name system must be accomplished through standards that are open, non-proprietary, and fully compatible with the Internet's existing end-to-end model and that preserve globally unique naming in a universally resolvable public name space."

More recently, on 16 April 2002, ICANN took the additional forward-looking step of publishing a "Discussion Paper on Non-ASCII Top-Level Domain Policy Issues".⁵⁵ This paper is intended to begin the discussion of issues relevant to the introduction of new TLDs which, like the IDN domain names discussed above, may themselves appear in a non-Latin-character script. In time, for example, we may expect that a non-ASCII TLD, consisting of Japanese characters

semantically associated with the recognized geographical unit of Japan (.jp), could be introduced into the DNS. As the Discussion Paper states, the ICANN IDN Committee's

"current thinking focuses on extending to the IDN namespace existing policies and concepts for the creation of ASCII generic TLDs (gTLDs) and ASCII country-code TLD (ccTLDs), which have been developed and refined over time, while giving due consideration to additions and variations in policy to take into account unique factors related to the use of non-ASCII characters within the DNS."⁵⁶

In addition, the Committee has generally agreed that the core purpose for introducing non-ASCII TLDs "would be to make the DNS service easier to use for Internet users whose native languages include non-ASCII characters."⁵⁷

These new developments for the DNS are timely. The Internet is rapidly evolving from its predominantly English language roots to reflect the creativity, expression, communication and business interchange which occurs in other languages. It is estimated that by 2007, Chinese will be the most common language used on the Internet. Such a development would merely reflect the nature of communications prevailing offline, in which 92 percent of the world's population speaks a primary language other than English.⁵⁸

While it is likely that it will still take time, the roll-out of IDN technology should provide significant benefit to developing countries, increasing the intuitive use of domain names and improving navigation of the Internet. As discussed above, there should also be opportunities to introduce new IDN top-level domains, which may become very popular within certain regions or countries. The policies to be associated with these new TLDs, as discussed in section B.2(b) above concerning ccTLDs, can be developed in a manner which is appropriate to the relevant governmental, legal, cultural or other requirements.

3. Competition in domain name registration services

ICANN has accredited a geographically diverse set of approximately 150 companies as competitive domain name registrars for the gTLDs (specifically for .aero, .biz, .com, .info, .name, .net and .org).⁵⁹ About 80 of them are currently operating to receive domain name registrations, while others are accredited but have not

yet commenced operations. A complete listing of accredited organizations is available on the ICANN website.⁶⁰

It is important that the overall structure of the domain name services market provide a competitive environment for companies offering services. The first-come first-served, highly automated and efficient nature of the registration system has allowed the tremendous growth that has taken place, while acting as the means of preserving universal connectivity on the Internet.⁶¹ Initially, however, just one company, Network Solutions, acted as both the registry and registrar for the popular .com, .net and .org gTLDs. Thus, Network Solutions was a single historical provider, which had enjoyed a monopoly granted by the United States Government over new domain name registrations and renewals.⁶²

With the separation of functions between registry and registrar, and the changes that have been brought about through the ICANN process over the last few years, the situation has evolved significantly, as noted above with the introduction of competition among registrars. At the same time, however, it is a widely held view that the registry function in the DNS for each TLD presents a natural monopoly situation (i.e. administering the centralized and authoritative database for the particular TLD), which cannot, from a technological perspective, be shared among competing companies. Thus, while some level of competition can be achieved among the registries for different gTLDs, there cannot be two companies to operate the database and carry out administrative functions for a particular TLD. The separation of the registry from the registrar functions has permitted competition at the registrar level among companies accepting domain name registrations from end-customers. Nevertheless, as more companies have become involved – some operating as TLD registries, others acting as registrars, and still others assuming both functions – the environment for competition within the DNS has become more complex. This is an area in which continued vigilance and oversight are required.

(a) ICANN accreditation

In order to become accredited by ICANN, a prospective registrar must satisfy a number of business, financial and technical requirements. These requirements are described in detail on ICANN's website.⁶³ The company must complete and submit an ICANN Registrar Accreditation Application, pay a non-refundable \$2,500 fee and eventually sign a Registrar Accredita-

tion Agreement with ICANN. The technical capabilities, for example, should be designed to ensure security and continuity, irrespective of whatever might happen to a particular registrar's business – this is vital to the stability of the Shared Registration System. Once accredited, the company will be required to pay annual accreditation fees of \$4,000 for the first and \$500 for each additional TLD in which it will be accepting domain name registrations. It will also be required to pay quarterly fees representing a contribution to ICANN's operating costs, which will be based on the registrar's share of overall domain name registrations in the TLDs for which it is accredited. An applicant will be required to demonstrate that it has capital of approximately \$70,000 or otherwise show that it has the financial resources necessary for carrying on the business.

An organization seeking to begin registrar operations will also be required to enter into several contracts with the operators of the gTLD registries. One of the reasons for this is the licensing of the proper technology (software) to allow interoperability between the registrar and registry operators. In addition, the registrar will be required to comply with various rules and requirements established by the registry operator (i.e. imposed through the chain of contracts mentioned above). For example, in dealing with VeriSign, the core agreement is the Registry-Registrar-Agreement (RRA).⁶⁴ This contract provides that registrars will pay VeriSign \$6 for each domain name registration and annual renewal. The registrar will also be required to provide payment security, which is used to secure the registrations that the registrar performs each month.⁶⁵

It is only after a prospective registrar has met all these requirements that it is allowed to begin operations. Thus, the technical, legal and financial requirements are not insignificant. The system appears to be working for the 80 registrars already in operation; however, if the volume of new domain name registrations as well as renewals declines, new stresses may be imposed on the system. Organizations which have been accredited by ICANN but are still not actually operating may be weighing the pros and cons of beginning registration services, in view of the additional costs that this step entails.

(b) Price competition for domain name registration services

In order to evaluate the competitive system for registrars, it is useful to review domain name market infor-

mation, as well as the prices that customers are being charged to register domain names.

Concerning the first issue, recent statistics show that the overall market volume for domain name registrations in the gTLDs (including multilingual domain names in the VeriSign test-bed) peaked in October 2001 at approximately 30,700,000 registrations, and has recently decreased to just under 30 million, despite the introduction of new gTLDs.⁶⁶ The slight decrease in total registrations, while not encompassing registration activity in the ccTLDs, is considered to be caused by a drop-off in the rate of new registrations, a smaller number of renewals and fewer defensive registrations.⁶⁷ The initial “boom” period for the domain name industry, which we have witnessed over the last five years, may now be waning.

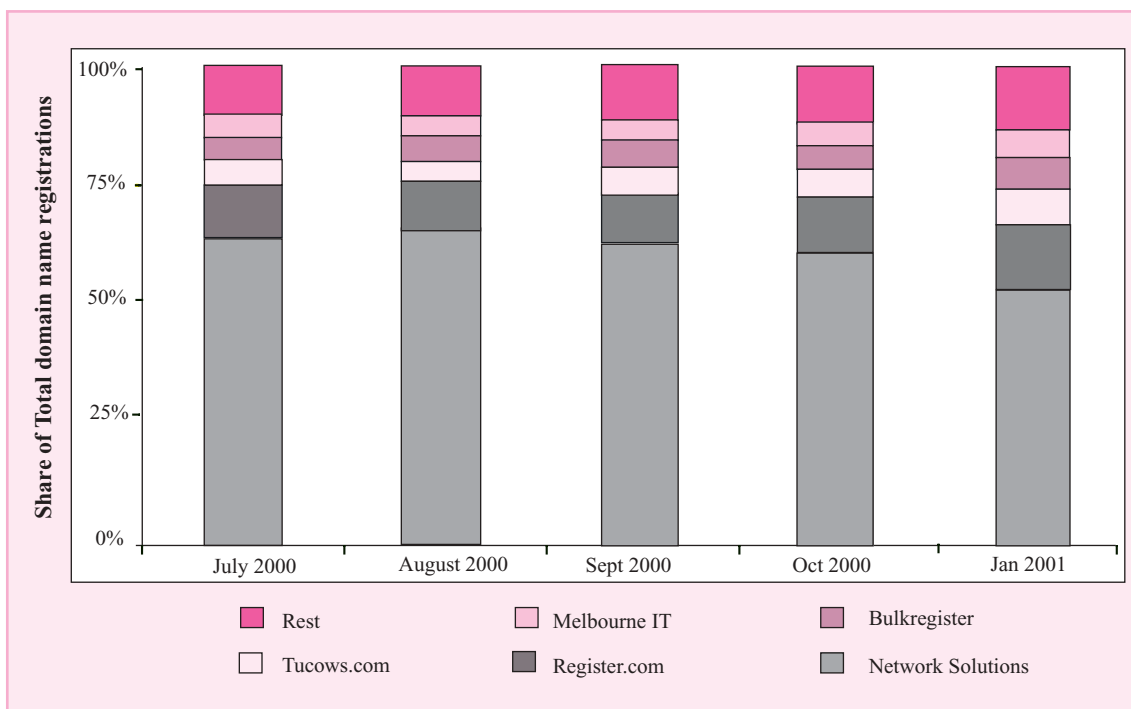
With respect to the restructuring that has taken place in the market for gTLDs – that is, introducing compe-

tion among domain name registrars – there have been significant results. VeriSign/NSI’s share of total domain name registrations in the gTLDs decreased from approximately 70 per cent of the market as of July 2000 to 50 per cent in January 2001 (chart 5), and further recent falls have also been noted.⁶⁸

In contrast, other ICANN-accredited registrars have gained a greater foothold in the market. For example, Register.com’s share increased over the same period, with an approximate share of 15 per cent in January 2001.

Regarding the prices charged by registrars to their customers, there are significant differences. The accredited registrars have implemented various business models in relation to their domain name registration activities. Some registrars concentrate only on domain registration or parking services, while others focus on marketing a more complete service, including hosting. Hosting the domain name can include, for example,

Chart 5
Share of total domain name registrations



Source: copyright: Matthew Zook (2001).

also providing data storage space for a web presence or e-mail services. These registrars might not charge the user for the registration of the domain alone because they are charging instead for an overall service. There is also no shortage of “free” domain hosting services which usually require the user to include advertising on its website. Finally, some registrars offer

periodic discounts, others offer volume discounts, and still others offer their registration services only to wholesalers.

With these variations in mind, the prices for registration of a domain name in the gTLDs may start at as low as \$9 per year, which is similar to the amount that

accredited registrars must pay to VeriSign for each domain name registered in the .com, .net or .org TLDs. Most, however, can be found to charge between \$15 and \$35.⁶⁹ In the ccTLD context, the fees for registration similarly reflect a range of prices. At one end of the spectrum, as in the case of the .cg ccTLD for Congo, registration of a domain name may be free of charge to citizens or lawful residents; at the other end, there are countries where registration can be relatively expensive, such as Togo, where a two-year registration costs \$270.

Table 11

Registrar charges, selected registration services in the .com domain (15 June 2002)

Registrar	Country	\$ domain/year
NSI/VeriSign	US	35
Register.com	US	35*
TUCOWS.com	CA	10**
BULKREGISTRER.com	US	10***
Melbourne IT	AU	35***
Go Daddy	US	9***

* Service includes e-mail address and three web pages.\$

** Whole registration service.

*** Members only, one time registration fee \$79.

Source: Ican.

While the domain name registration process appears to be increasingly competitive, there are other areas, such as registry services, where competition is now being introduced, but only in the form of new gTLD registries as alternatives to the .com, .net and .org gTLDs operated by VeriSign. As noted above, there may not always be a strict separation of registry and registrar functions, and this too can lead to competition concerns in relation to whether a given registry, which may also act as a registrar for its TLD, will obtain any unfair advantage, particularly when it has agreements with other companies that are also acting as registrars to receive registrations in the same TLD.

Domain names have increased considerably in market value. A whole new industry of intermediaries has emerged to appraise domain names, in some cases using the appraisal to resell the names directly, while in other cases providing the appraisal to a third party.⁷⁰ One way may question whether companies that act to merely snapup and resell popular domain names at

Table 12

Registration fees, selected African ccTLD registration services in geographical order from North to South

ccTLD	Country	Appr. \$ Domain/year Initial registration fee
.ly	Libyan Ara Jamahiriya	500*
.sn	Senegal	free
.mr	Mauritania	free
.gh	Ghana	50
.ke	Kenya	200
.ug	Uganda	50
.mw	Malawi	140

* Registration of third-level domains available at cheaper rate.

Source: Alridns.org

premium add any value to the industry or to consumers. Aside from some of the legal (e.g. intellectual property) issues that can arise in the context of domain name resales, however, there can be other concerns. For example, registrars, attracted by the high prices that have been paid for certain domain names, may seek to identify high-value names and take them or otherwise exclude them from the first-come-first-served registration process, in order to sell them at a much higher price to interested customers. A well-designed competitive system seems to be the best way to avoid any such activities. The operation and control of the registry is of major importance in this context: any retired or deactivated domain name must be subject to the random and competitive registration process in which all accredited registrars participate on a fair and transparent basis.

Table 13

Highest reported prices for domain names

Business.com	11/99	\$7 500,000
AltaVista.com	07/99	\$3 250,000
Loans.com	01/00	\$3 000,000
Wines.com	09/99	\$3 000,000
Autos.com	12/99	\$2 200,000
Express.com	12/99	\$2 000,000
WallStreet.com	04/99	\$1 030,000
eFlowers.com	02/99	\$1 000,000
Forsalebyowner.com	01/00	\$835,000
Drugs.com	08/99	\$823,456
Cinema.com	02/00	\$700,000

Source: domainstuffet.com

C. The role of ICANN

Frequent reference has been made throughout this chapter to ICANN, the Internet Corporation for Assigned Names and Numbers. ICANN has become a central player in the management of the DNS, with its governance and coordinating functions extending to many areas of importance for the global Internet infrastructure. However, while it has taken a number of important measures and achieved a number of important successes, it has not been able to avoid continuing questions concerning its structure, basis for legitimacy and authority, funding and international representativeness.

ICANN was formed in 1998 as a private sector initiative to assume responsibility for overseeing the technical coordination of the DNS. There was a sense at that time that the growing international and commercial importance of the Internet necessitated the creation of a technical management and policy development body that was more formalized in structure, more transparent and accountable, and more reflective of the diversity of the world's Internet communities; this contrasted with the early ad hoc and voluntary efforts to coordinate the functions of the DNS. Rather than establish an international treaty-based organization, which might have been the means used in the past to create an entity with oversight of a global medium, a new model was followed. Internet management has generally been based on the principles of non-interference, self-management and self-regulation. In keeping with this trend, ICANN was set up as a non-profit, private sector corporation⁷¹ formed by a coalition of the Internet's technical, business, academic and user communities. ICANN has achieved recognition and received regular input from a number of governments, including those serving on the ICANN Government Advisory Committee (GAC).⁷² Nevertheless, it continues to face calls for reform, which consistently raise fundamental questions as to its legitimacy, representativeness, the scope of its authority and appropriate processes for formulating policy.

ICANN states that it has the "objective to operate as an open, transparent, and consensus-based body that is broadly representative of the diverse stakeholder communities of the global Internet".⁷³ In a phased process with assistance from the United States Government, which funded much of the early development of the DNS, ICANN has been assuming responsibility for coordinating the stable operation of the Internet in four key areas:

- The Domain Name System (DNS);
- The allocation of IP address space;
- The management of the root server system; and
- The coordination of protocol number assignment.

As discussed above, ICANN has been funded through the registries and registrars participating in the global DNS. While maintaining a small staff and a volunteer Board of Directors,⁷⁴ ICANN has worked to achieve consensus for its policies through a representative structure composed of three supporting organizations – the Domain Name (DNSO), Address (ASO) and Protocol Supporting Organizations (PSO). Each of these organizations has its own membership and, collectively, they are intended to represent the interests of a broad cross-section of the global Internet's business, technical, academic, non-commercial and user communities. Among ICANN's achievements since 1998, it has developed and launched the system of competitive registrars, implemented a Uniform Dispute Resolution Policy (UDRP) to deal with domain name disputes (discussed below) and introduced seven new gTLDs. On the technical side, ICANN has performed the IANA address allocation and protocol numbering functions and taken over the operation of one of the DNS root name servers.

Despite this progress over the last four years, the critical questioning concerning ICANN's proper role and organization surfaced again earlier this year. The work of the three supporting organizations, and particularly the DNSO, has not proceeded smoothly, but has been accompanied by a constant set of challenges. On 24 February 2002, the President of ICANN, Dr. Stuart Lynn, posted a report entitled "ICANN – The Case for Reform". This was followed by another one, published on 10 March 2002 and entitled "Toward a Statement of the ICANN Mission". In his report, Dr. Lynn emphasized that ICANN, despite its progress, still faces serious issues:

"ICANN is still not fully organized, and it is certainly not yet capable of shouldering the entire responsibility of global DNS management and coordination. ICANN has also not shown that it can be effective, nimble, and quick to react to problems. ICANN is overburdened with process, and at the same time underfunded and understaffed. For these and other more fundamental reasons, ICANN in its current form has not become the effective steward of the global Internet's naming and address allocation systems

as conceived by its founders. Perhaps even more importantly, the passage of time has not increased the confidence that it can meet its original expectations and hopes”.

The report grouped ICANN’s major problems into three categories: too little participation by critical stakeholders (across the full range of infrastructure operators, major users and national Governments); too much focus on process; and too little funding to support quality services.

Among particular concerns, and an issue that has special relevance for developing countries, the report noted that most administrators of ccTLDs have yet to sign any formalized agreement with ICANN, such as the Model ccTLD Sponsorship Agreement discussed above, which would define the rights and responsibilities of each party. To date, only two countries – Japan and Australia – have signed these sponsorship agreements.⁷⁵ Most other ccTLD administrators have cooperated with ICANN policies only on a voluntary and informal basis. The ccTLD constituency group within ICANN has advanced its own model contract for ICANN’s consideration, to which ICANN has not agreed. Reflecting ongoing tensions in this area, the ccTLDs, as a group, have further contended that they should have standing to form their own ICANN supporting organization, to be considered on an equal footing with the DNSO, ASO and PSO – as opposed to the current situation in which ccTLDs are only one constituency within the DNSO.

In June 2001 at ICANN’s meeting in Stockholm, the ccTLDs voted unanimously to withdraw from the DNSO and to form a new supporting organization, the “ccSO”.⁷⁶ Discussions continue within ICANN concerning the proper recognition, role and level of participation of ccTLDs within ICANN. The circumstances involving ccTLDs within ICANN, including contribution to ICANN’s funding, are clearly among the issues that must be considered in any ICANN reform effort. ICANN must properly address the role of ccTLDs, and make further outreach efforts while at the same time respecting the ccTLDs independence. ICANN must continue to find measures that will secure their voluntary participation in the ICANN system.

Dr. Lynn’s report indicated that structural reform, not mere tinkering, was needed to overcome the problems he identified:

“I have concluded that ICANN needs reform: deep, meaningful, structural reform, based on a clearheaded understanding of the successes and failures of the last three years. If ICANN is to succeed, this reform must replace ICANN’s unstable institutional foundations with an effective public-private partnership, rooted in the private sector but with the active backing and participation of national governments.”

He also recommended a more professional, more broadly representative and more expert Board of Directors, which must be given explicit responsibility for managing the policy development process, and must seek to work more closely with Governments in doing so. He suggested new procedures for nominating Board members. At the same time, he stressed that ICANN should remain an organization that seeks to identify and implement consensus solutions, while being led by the private sector, not Governments.

Following the President’s report, the ICANN Board established a Committee on ICANN Evolution and Reform. This Committee has instituted a consultation process, calling for comments on a number of key issues, including:

- What should ICANN’s mission be?
- Are the issues raised in the report a correct perception of the problems facing ICANN?
- Assuming that structural and procedural reforms are necessary in order to ensure that ICANN carries out its mission, what transition mechanisms or approaches should be used to migrate from the status quo to the future environment?⁷⁷

Particular topics to be considered by the Reform Committee include:

- ICANN’s at-large membership and participation;
- The appropriate means and level of participation by Governments;
- Funding levels and mechanisms;
- Proper ICANN policy-formulation bodies (i.e. the proper constitution and role of supporting organizations and other advisory committees);
- A nominating committee for the Board.

Recently, the former chairperson of the ICANN Board of Directors, Esther Dyson, acknowledged that ICANN is “mired in disputes about authority, accountability and openness”. She has suggested that “the US Commerce Department should step in to establish standards to adjudicate disputes if ICANN is unable to solve matters in the next six months”.⁷⁸ A number of civic groups, led by the Media Access Project, are even calling for the United States Government to reconsider its 1998 selection of ICANN as a private, non-profit organization to take over responsibilities for the DNS. Meanwhile, a Senate committee held hearings in June, and the investigative arm of the Congress has questioned ICANN’s legitimacy and effectiveness.⁷⁹

As of the date of this Report, the ICANN reform process continues. At its meeting in Bucharest in June 2002, the ICANN Board approved a “Blueprint for Reform” which recommends a new management structure and procedural change for ICANN.⁸⁰ The Board requested that the ICANN Evolution and Reform Committee (ERC) oversee the detailed implementation of the Blueprint. Among the priorities listed was to “devise and incorporate specific measures to ensure, to the extent feasible, geographic and cultural diversity in all parts of ICANN structure”.

The ERC has moved forward very quickly with its work on reform. A number of status reports on all aspects – including ICANN’s mission and core values, structure, accountability and funding – have been put forward.⁸¹ The ERC will make available its final recommendations in October 2002, to be considered by the ICANN Board at its meeting in Shanghai on October 27-31, 2002.

For developing countries, the reform of ICANN is an important issue, one which should be closely followed. ICANN remains a key institution for coordinating the technical management of the DNS, and a forum where developing countries can become more involved and learn more about the DNS. However, the important questions of reform must be carefully addressed, so that ICANN can build a new mandate and refocus its efforts. Although not a treaty-based organization, ICANN seeks to serve a similar role, managing the DNS as a public good for all. Developing country representatives, acting at a governmental level and at the level of the ccTLD manager, can provide important input on issues involving ICANN’s mission, participation of stakeholders and methods for formulating policy. Importantly, developing countries can contribute their views on what mechanisms

might best serve to promote international participation and a more international outlook for ICANN.

ICANN, although short of funds, has made outreach efforts towards developing countries. For example, it has held a number of its public meetings during its four years of existence in developing countries, including Chile, Egypt, Ghana and Uruguay. Meetings in 2002 are due to take place in Romania and China. ICANN, however, has not had the resources to be able to operate in more than one language (i.e. English), nor has it established any working groups specifically responsible for promoting and expanding a general understanding of the DNS and ICANN’s activities in developing countries. New initiatives by developing countries could promote changes in these and other important areas. At the same time, it is clear that there is presently insufficient funding for ICANN to financially assist in the participation of delegates from developing countries.

As this discussion demonstrates, ICANN and its mandate continue to evolve. Developing countries, either directly or acting through the regional ccTLD organizations described above, should engage in the ICANN process so that their perspectives, requirements and diversity are taken into account.

D. Domain names and legal issues: The relationship between the DNS and intellectual property rights

Domain names have generated a number of legal issues, aside from the contractual arrangements discussed above which establish a chain of agreements defining rights and responsibilities among the DNS players. Foremost among such other issues is the tension arising from conflict between domain names and the existing legal system for protecting trademark rights. The registration and the use of trademarks, which create an exclusive legal right for an owner to use a mark, have fostered confidence in national and international markets by allowing marks to be uniquely associated with a particular company or brand, and by protecting both the public and the mark owner from fraud and deception. Relying on trademark law, a company can develop goodwill in its brand and expect that it will be protected from infringing imitators. At the same time, consumers can gain confidence in particular companies or brands and be protected from the same deceptive practices. Trademarks are important in both developed and developing countries.

Domain names, as we now understand, were launched into the commercial space in a manner that disregarded the existing intellectual property system. A simple, quick and largely automatic process for registering a domain name through a website, first utilized for the gTLDs .com, .net and .org but now commonly applied in many gTLDs and ccTLDs, created conditions for a wave of registrations of popular names. And the domain name registrars – the companies actually registering the names – had every incentive to allow these registrations to continue, thus creating a veritable money machine for their businesses. One positive consequence of this highly automated approach to domain name registrations is that it has presented a low entry barrier for the many new entrants to the e-commerce marketplace, including businesses in developing countries, as they could cheaply and easily register a distinctive name corresponding to their business or brand name. At the same time, however, a group of self-styled “entrepreneurs” have registered thousands of names through automated websites, including generic words as well as names corresponding to trademarks, in order to sell the registration to third parties at a profit. Where a trademark is involved, this has become known as the practice of **cybersquatting**.

Unlike the quick and automated approach for registering domain names, the intellectual property system is administered by public authorities on a territorial basis, creating rights within the territory concerned, in particular for trademarks in relation to certain categories of goods or services. Obtaining a national trademark from the relevant public authority remains a slow and more costly process. The complete disjunction between these two systems has thus given rise to practices that include the deliberate, bad faith registration of trademarks as domain names in order to sell the domain names to the owners of those marks, or simply to take unfair advantage of the reputation attached to the marks.

The incentives for this type of practice existed in particular early on because:

- (a) The domain name registration system is based on a simple first-come-first-served practice;
- (b) There were no rules in the system that would prevent the “resale” of the names at any price; and
- (c) There were no clear legal precedents indicating that the targeting of trademarks through regis-

tration of a domain name was an unlawful practice.

All of this, of course, has changed dramatically, although not without passing through a somewhat painful transition in which trademark owners and domain name registrants, and various other stakeholders involved in the Internet, have battled to draw the lines that should apply to delimit fair as opposed to abusive practice.

While the earliest legal precedents establishing fair versus abusive practice were decided in the courts, a significant contribution was made in a study carried out by the World Intellectual Property Organization (WIPO), based in Geneva, entitled “The Management of Internet Names and Addresses: Intellectual Property Issues”.⁸² WIPO was requested by its member States in July 1998 to study the intellectual property issues associated with domain names and develop relevant recommendations. This study, also known as The Report of the WIPO Internet Domain Name Process (“WIPO Report”), was published in April 1999 after an international consultation process. It proposed a number of recommendations to ICANN on methods for dealing with these and other intellectual property issues arising out of the registration of domain names. The recommendations included:

- **Best practices:** the adoption of improved, standard practices for registrars, in particular in relation to enhanced registration agreements with domain name holders and requiring that they supply accurate contact details. Where it is shown that contact details are inaccurate and do not enable contact with a domain name holder, the registrar should have the right to cancel the domain name registration. This recommendation was implemented through the accreditation requirements established for registrars by ICANN. One of the other legal issues – aside from intellectual property – that arises as a result of the availability of contact details for domain name registrants is concern for protection of privacy, which is discussed below.
- **Exclusions for famous and well-known marks:** it was recommended that, because famous and well-known marks have been a special target of cybersquatters, a mechanism could be introduced whereby the owner of such a mark can obtain an exclusion in some or all gTLDs, prohibiting anyone other than such owner from registering it as a domain name.

This recommendation was never taken up by ICANN.

- **Controlled introduction of new gTLDs:** it was recommended that any new gTLDs should be introduced cautiously and slowly, permitting assessment from the perspectives of stability of the Internet and the intellectual property community. In fact, ICANN has implemented seven new gTLDs, as described above. It has sought to implement a careful and robust process for the implementation of these new TLDs. Nonetheless, their implementation has been accompanied by problems.
- **Administrative dispute resolution procedure:** it was recommended that a mandatory dispute-resolution policy be adopted under which registrants in all gTLDs submit to a uniform administrative procedure for trademark disputes arising out of the registration of their domain names. Following on from this recommendation, ICANN adopted the Uniform Domain Name Dispute Resolution Policy (UDRP), which is discussed at length below.

Of these four WIPO recommendations, the proposal for a new and international dispute resolution policy – the UDRP – has had the greatest significance in the DNS. Before discussing the UDRP, however, it will be useful to review four primary methods by which disputes involving domain names can be resolved: (a) negotiation between parties; (b) mediation; (c) arbitration or similar administrative procedures; and (d) litigation.

There are many circumstances in which, although a claimant might have a strong legal position, it would nevertheless be more practical to buy the name from the registrant at an agreed price. For example, so long as the cost of purchasing the name is cheaper than the alternative means of seeking to obtain the name, practical negotiation might be preferred. This approach can also be less risky than awaiting an uncertain adjudicated decision, and may be a first step before such other measures are contemplated. Mediation, on the other hand, has not generally been perceived as a suitable solution for domain name disputes, particularly when the registration is considered to be abusive. It can, however, be useful to parties disputing in good faith who are unable to come to an agreement among themselves, but are nevertheless willing to negotiate with the assistance of an independent neutral – i.e. the mediator – to find a mutually acceptable solution.

Nominet UK, the operator and registry for the .uk ccTLD, provides informal mediation services for domain name disputes as a preliminary step before escalating the dispute to Nominet's own adjudicated dispute resolution procedure, the Nominet Dispute Resolution Service, which is modelled on the UDRP.

Procedures modelled on arbitration are proving to be perhaps the most effective way of resolving domain name disputes. As noted below, the UDRP follows an arbitration model of semi-private adjudication, although the decisions in these cases are publicly posted. For many individuals and entities, this arbitration model is a feasible and cost-effective method for resolving disputes in a short period. This may be particularly true for businesses and individuals from developing countries. Litigation, in contrast, is generally considered to be the most expensive and lengthy process for resolving a domain name dispute. This is due to court procedural requirements and deadlines, and the likely need to hire local counsel, as well as possible congestion in certain court systems. These factors can combine so that a dispute will drag on for many months at significant cost to the parties involved. High costs can be a disadvantage to businesses and individuals in developing countries. The cost of dispute resolution procedures becomes a key element, among several others, in evaluating the fairness of an international system for resolving domain name disputes.

Finally, it should be noted that various mechanisms have been established to avoid disputes before they arise, such as limited pre-screening prior to registration, or "sunrise" periods during which only trademark owners can register – for example, Afilias established a sunrise period for the .info TLD.⁸³ Although a laudable objective for avoiding disputes, these efforts have themselves generated further issues and consequences.⁸⁴

1. Uniform Domain Name Dispute Resolution Policy (UDRP)

The UDRP was adopted by ICANN and went into effect on 1 December 1999, applying to domain name registration in the gTLDs. Modelled on recommendations made by WIPO, it provides trademark holders with an administrative mechanism for the resolution of disputes arising out of the bad-faith registration and use by third parties of Internet domain names corresponding to their trademarks.

When it was introduced there was some uncertainty as to whether the new UDRP procedure would be widely used by trademark holders to assert their rights. In particular, during the consultations of the WIPO Domain Name Process, some comments were received from groups at both ends of the debate spectrum – that is, representatives of trademark holders as well as Internet groups asserting the rights of domain name holders – to the effect that the creation of a new international forum for resolving such disputes might not gain the trust of these parties and would therefore not be extensively used. However, on 2 December 1999, the first day after the UDRP was adopted, the answer to this uncertainty gradually started to become clear. The WIPO Arbitration and Mediation Center received the first domain name complaint filed under the UDRP, and some six weeks later, a panellist appointed by the WIPO Center decided that the domain name at issue, <http://worldwrestlingfederation.com>, was to be transferred to the complainant, the World Wrestling Federation Entertainment, Inc.⁸⁵ For parties from developing countries, the UDRP offers an internationally accessible dispute resolution forum, but as with any legal procedure, parties must be well informed about their rights as well as about the requirements of the procedure itself.

Since the commencement of the UDRP approximately two and a half years ago, more than 6,100 cases have been filed under the procedure. This is a significant number of disputes to be submitted in a short time to a new forum applying new procedures. While most commentators have expressed positive views concerning the UDRP, there have been issues raised by some, which are discussed below, about the overall fairness of the procedure, particularly as regards domain name registrants.

(a) Review of the UDRP procedure

ICANN introduced the UDRP and an accompanying set of procedural Rules,⁸⁶ and further determined that multiple dispute-resolution service providers, which ICANN would periodically accredit, would administer the uniform procedures. As a result, trademark holders can submit complaints to the following dispute-resolution providers for disputes involving domain names that have been registered by an ICANN-accredited registrar:

- Asian Domain Name Dispute Resolution Centre (ADNDRC), approved effective 28 February 2002, with offices, in Beijing and Hong Kong (China),⁸⁷
- CPR Institute for Dispute Resolution (CPR), approved effective 22 May 2000,⁸⁸ located in New York;
- eResolution (eRes), approved effective 1 January 2000; no longer accepting proceedings commenced after 30 November 2001 and now out of business;
- National Arbitration Forum (NAF), approved effective 23 December 1999,⁸⁹ located in Minneapolis;
- World Intellectual Property Organization (WIPO), approved effective 1 December 1999⁹⁰, with its office in Geneva.

As indicated above, the ADNDRC is the provider most recently approved by ICANN, and it will offer enhanced accessibility to the Asia-Pacific community.

The UDRP procedure is a uniform procedure, which means that the same rules for decisions and procedures are to apply no matter which of the dispute resolution providers handles a complaint. This uniformity also works to enhance a general understanding of the UDRP, which can be of benefit to all parties wherever they are located, be it in developed or developing countries. The procedure is optional for trademark owners: they may choose to use the UDRP or they may go to court. Domain name registrants, by contrast, must agree in their registration agreement to submit to the UDRP procedure, once a complaint has been filed concerning a domain name registered by them. The UDRP is limited to cases of bad-faith registration and use. Cases between parties alleging competing legitimate rights to names are therefore excluded.

For a complaint to be successful under the UDRP, the complainant must establish that the following three cumulative criteria are satisfied:

- (a) The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- (b) The registrant of the domain name has no rights or legitimate interests in respect of the domain name; and
- (c) The domain name has been registered and is being used in bad faith.⁹¹

The complainant must demonstrate and prove that all three of the above elements are present.⁹² Further

guidance as to what constitutes evidence in bad faith registration and use of the domain name⁹³ is provided in the UDRP. These illustrative circumstances include the following:

- (a) The registrant has acquired the domain name primarily for the purpose of selling, renting or otherwise transferring it to the complainant who is the owner of the trademark or service mark, or to a competitor of the complainant, for valuable consideration in excess of the “out-of-pocket” costs directly related to the domain name;
- (b) The registrant has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that a pattern of such conduct is evidenced;
- (c) The domain name has been registered primarily for the purpose of disrupting the business of a competitor; or
- (d) The domain name has been registered primarily for commercial gain through creating the likelihood of confusion.

In defence of its registration, a domain name holder – referred to as the respondent under the procedure – can demonstrate its rights or a legitimate interest in a domain name by presenting evidence that:

- (a) Before any notice to the respondent of the dispute, the respondent used, or prepared to use, the domain name or the name corresponding to the domain name in connection with a bona fide offering of goods or services;
- (b) The respondent has been commonly known by the domain name, even if the trademark or service mark rights have been acquired; or
- (c) Legitimate non-commercial or fair use of the domain name, without intent to divert consumers or tarnish the trademark or service mark for commercial gain, is being made.⁹⁴

A respondent can further allege “reverse domain name hijacking” that is, that the complaint was brought in bad faith, i.e. primarily to harass the domain name holder. If the panel agrees, it may declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.

To begin a case under the UDRP, the complainant must submit a complaint to one of the

ICANN-approved dispute resolution service providers. Model forms for the complaint (and response) are available from each service provider through its website. The complainant must specify whether the dispute is to be decided by a single- or three-member panel. If the complainant requests a single-member panel, the respondent has the right to indicate in its response that it would choose to have the dispute decided by a three-member panel instead.⁹⁵ The fee for a single-member panel is paid entirely by the complainant – this is an important cost factor built into the design of the UDRP.⁹⁶ However, if the complainant has elected to have the dispute decided by a single-member panel and the respondent requests a three-member panel, the respondent is then required to pay half of the applicable fee for the three-member panel.⁹⁷

Once the service provider has received the complaint and confirms that it complies with the requirements of the UDRP and the service provider’s supplemental rules, it is then forwarded to the respondent.⁹⁸ The respondent must provide a response to the complaint within 20 days.⁹⁹ If the respondent fails to respond, the panel will decide the case on a “default” basis, reviewing only the information and evidence furnished by the complainant.¹⁰⁰ Following receipt of the response (or after the 20 day period has elapsed), a decision should be issued by the panellist two weeks later, unless there are exceptional circumstances.

The UDRP procedure is relatively simple because the remedies available are restricted to:

- Transferring the domain name registration;
- Cancelling the domain name registration; or
- Rejecting the complainant’s claim, in which case the domain name registration remains with the respondent.

Monetary damages in particular are excluded under the UDRP, as is the award of any costs associated with the procedure.¹⁰¹

Once a UDRP decision is notified by the dispute resolution service provider to the registrar that handled the registration of the domain name in dispute, that registrar is obliged to implement the decision. This required enforcement, for example to transfer the domain name registration from the respondent to the

complainant, will take place ten days after the panel decision has been notified, unless the respondent files a court case against the complainant within that period and provides a copy of the court complaint to the registrar. By assuming the key role under the UDRP of implementing decisions notified to them, registrars reap a significant benefit: they avoid being joined directly as parties in the dispute itself. Questions of direct or indirect infringement are no longer of serious concern to registrars, so long as they carry out their responsibilities within the ICANN system and, in particular, under the UDRP. The direct enforcement of UDRP decisions by registrars also lightens the burden on parties located internationally to obtain the intended result under the procedure without needing to go to court merely to enforce a UDRP decision.

(b) Responsibilities of UDRP dispute resolution service providers

One of the significant challenges faced by the dispute resolution service providers implementing the UDRP has been not only to achieve acceptance of this novel administrative procedure, but also to encourage parties to use the procedure in an online manner. Given the nature of the disputes (i.e. who has rights to a particular domain name that is to be used as an Internet address), it is reasonable to assume that parties will have some technical sophistication and access to technology. At the same time, however, consideration must be given to the likely international spread of the parties using the UDRP system, many of whom might speak different languages and operate in different business and legal cultures, and some of whom would face significant technical bandwidth constraints. These are real concerns which test the effectiveness of the procedure, particularly for parties located in developing countries.

The service providers addressing these challenges have had to adopt approaches that are appropriate for the broadest possible constituency – some have done a better job than others. Since the process takes place online, the dispute resolution provider's website itself should be extremely reliable, meeting the requirements of an audience that requires international access and service. In addition not only the UDRP procedures but also the dispute resolution providers' administrative services should be broadly transparent. Thus, a provider's website should present the procedure as largely self-explanatory by providing complete information, including the source documents, guides, model forms, notices of pending cases and full texts of published decisions. The accredited dispute resolution

providers have so far done a good job of meeting these aims. Furthermore, the website, if at all possible, should provide this information in a multilingual presentation to meet the needs of parties around the world – the ADNDRC and WIPO for example, provide services and information in languages other than English. Finally, with respect to technology, the provider's systems should use only commonly available tools, such as a website accessible using the common browsers, e-mail with attachments in multiple formats, and support and answers to questions by telephone, when necessary.

(c) Analysis of the UDRP

It is remarkable that the international forum established by the UDRP, and the online dispute resolution services offered thereunder, both of whose viability was questioned early on, have met with widespread and international acceptance. Complainants entrusting their cases to the UDRP now include internationally recognized businesses from every sector of commerce. Moreover, many smaller enterprises and individuals from different countries have also used the UDRP. Reflecting the international reach of electronic commerce, the parties filing or defending cases have come from more than 70 countries on every continent. Under the ICANN Rules, procedures have been conducted mostly in English, but also in Spanish, French, German and Japanese, with other languages to follow.

The use of electronic communications has allowed parties to participate according to their own schedule, rather than concern themselves with rushing a paper submission to the court-house steps. The automatic enforcement of decisions by accredited domain name registrars, once the required 10 day period has passed, avoids the need to seek enforcement of UDRP determinations in national courts. These measures, combined with the uniform set of procedural rules providing the framework under the UDRP, enable the dispute resolution service providers to administer cases from beginning to completion – on average, within two months of the filing of the complaint. The decisions are posted on the Internet by ICANN and the dispute resolution providers. The success of the UDRP so far owes much to the efficiency of these procedures and to the direct enforcement of the resulting decisions.

The international procedure also avoids the need to hire local counsel and to understand the local court rules and procedures (often a necessity in international

litigation). The UDRP itself lays down the three criteria for decision, and allows panellists in particular cases to make reference to any rules or principles of law that may be deemed relevant. A party can choose to represent itself, or to be represented by a lawyer who is able to carry the case from its commencement to decision. Travel is not required in order to prosecute a case: the procedure envisages that physical in-person hearings will be held only in the case of an exceptional matter, and so far it appears that no hearings have been held for any of the cases filed.

The relative simplicity of the system also extends to the schedule of fees. As noted above, the costs of the procedure are borne by the complainants (unless the respondent requests a three-member panel), who pay a fixed amount that covers both the dispute resolution providers' services and the remuneration of the administrative panel. This element is important, and takes into account the fact that domain name registrants might not be in a position to cover substantial expenses associated with the procedure. The actual

level of the fee depends on the number of domain names joined in a single dispute and on whether the case is to be decided by a single-member or three-member panel. The procedure appears to result in significant gains in efficiency while enabling a reduction in costs.

Perhaps in the light of this increased efficiency, one may ask whether the UDRP accords with accepted notions of due process for all the parties concerned. This is obviously an important question, and one that has been the subject of debate, particularly in the light of certain well-publicized decisions, among those following developments for this new administrative forum. Complainants have prevailed in approximately 80 per cent of the decided cases, securing the transfer of the domain name(s) in question.¹⁰² This high rate of decisions favourable to the complainants has also raised questions among commentators.¹⁰³ A number of commentators have voiced concerns about the UDRP, which are summarized in box 3.

Box 3

Critique of UDRP

- The system is said to promote forum shopping by complainants among the accredited dispute resolution service providers.¹⁰⁴
- Respondents are given insufficient time to respond (i.e. the 20-day period for filing a response).
- Panel composition (i.e. a one- or three-member panel) is a factor influencing case outcomes. Single-panel cases constitute approximately 90 per cent of the total caseload, while three-member panels comprise the remaining 10 per cent. Complainants win approximately 80 per cent of the time where a single panellist is appointed, compared with 60 per cent when a three-member panel is responsible for the decision.
- There is a lack of transparency regarding appointment of panellists in single-member cases.
- The decisions themselves are inconsistent and sometimes poorly reasoned.
- There is an absence of quality control mechanisms – i.e. appeal – built into the system.

These concerns have elicited thoughtful responses in the ongoing discussions concerning the UDRP. A significant study by the Max Planck Institute addressed a number of these concerns, including that the system “might be misused by rightholders, in particular big companies, in order to obstruct the selection and use of domain names by small business and private parties”.¹⁰⁵ The Max Planck study found that:

“as a matter of principle, the UDRP is functioning satisfactorily. No major flaws have been identified in the course of the evaluation”.¹⁰⁶

At the same time, the study confirmed that “considerable differences exist with respect to the outcome of decisions handed down” by one of the providers, eResolution, as compared with the National Arbitration Forum and the WIPO Arbitration and Mediation Center. Another commentator has explained that this difference could be due to the larger number cases in which three-member panels have acted to issue decisions administered by eResolution.¹⁰⁷ One would normally expect these cases to be more highly contested and not the outcome of non-contested default proceedings.

The Max Planck study identified four areas in which application of the UDRP was unclear and where further consideration could be given:

- The conditions under which a domain name is found to be “confusingly similar” with a trademark;
- Measures to be taken in order to safeguard the interests of free speech;
- Rules concerning the burden of proof and the standards to be applied in the assessment of the parties’ contentions; and
- The possibility of an appeal against UDRP decisions and how this could be incorporated in the UDRP framework.

Forum selection: With respect to the issue of forum selection raised above, it is clear that most complainants choose to submit their claims to the WIPO Center. A number of factors, other than the “win” percentage, can be important in explaining this choice. WIPO was the first accredited provider in the UDRP system, and provides an useful presentation of information on its website. Until recently, WIPO was the only dispute resolution service provider outside North America, and it offered its services and administered its cases in a number of different languages. It was responsible for the First Domain Name Report, which led to the adoption of the UDRP, and this factor too could be influential as regards the trust that has been placed in WIPO, not to mention the fact that it is a United Nations specialized agency. Its member States have been fully supportive of its role in administering domain name cases.

At the same time, the UDRP was indeed designed to give the complainant the choice of provider when submitting a claim. One might ask whether this was a wise policy, but it is not too dissimilar to other dispute resolution contexts, in which the plaintiff chooses the forum in which it will seek to prosecute its case. One commentator recently addressed these issues as follows:

“The UDRP procedure is far from perfect, but it is not unfair. No fair minded person could honestly believe that a provider would risk its reputation by selecting panellists who would decide cases in a pre-determined way. No panellist could hope to uphold her reputation, if she were to find for one party regardless of the law or the facts. Indeed, such conduct would be so transparent that users would lose

all confidence in the process. Clearly, this has not happened.”¹⁰⁸

High rate of success among complainants: With regard to complainants’ high rate of success, it should be considered that UDRP cases are submitted by complainants to any of the providers on the basis of an assessment of whether the complainant believes it has a good chance of success. There is a key element of ‘self-selection’ at the outset, which should also be viewed as responsible, at least in part, for the rate of success among complainants in general. The factual dispute centring on whether a domain name registration should be considered abusive presents a relatively uncomplicated set of circumstances, compared with the multidimensional factual disputes that can arise in other contexts of commercial litigation or arbitration. The UDRP itself excludes any consideration of monetary damages. Furthermore, the UDRP sets out bright line criteria for decisions about which factual circumstances will be considered an abusive registration, which prospective complainants can review before deciding whether to file a case. This greatly simplifies the situation, and also accounts for the fact that so many of the UDRP cases are uncontested and proceed on a default basis.

Given the clearly stated UDRP criteria for abusive registration, and the growing collection of precedents which are available for review online, a legal adviser can counsel a client against filing a case under the UDRP if the factual basis for cybersquatting is not apparent. As noted above, the adviser may propose, for example, that negotiation to purchase the name is a more realistic approach, and a safer course overall in terms of managing the trademark owner’s rights. This self-selection among the cases that are filed is an important element in the analysis of UDRP decisions and the prevailing high rate of success.

Time limit for response: It is also said that the UDRP imposes difficult time limits for respondents to be notified of, and to have time to respond to, a complaint brought against them. Developing countries may be affected by this in that there may be language barriers or difficulty in accessing the Internet to read e-mails and find out about a complaint, or understand the procedure in time. However, the UDRP states that the 20-day period may be extended either in exceptional cases or if parties mutually agree to extension.¹⁰⁹ The appropriate time for allowing the respondent to submit a response must be weighed against the overall time frame of the procedure – which is 45-60 days. Within this context, an additional

5-10 days for the response, given that it is the single submission to be provided by the respondent, may be appropriate.

UDRP appeals: The UDRP does not have an appeals mechanism. Part of the reason for this is to maintain the entire process of resolving domain name disputes as a fast, cost-effective and efficient process, which in turn makes it a more widely accessible system. The cost of filing a claim under the UDRP is currently reasonable on an international basis, even for parties in developing countries. If an appeals system is added in to the system, it may improve the quality of the decisions, but it will also add to the expense for many who might then have almost no other affordable way of filing a legitimate claim (this extra expense, however, might be limited to the appeal level only). Determining the proper constitution of an international appeal panel would also be a very difficult task. At present, given that the UDRP is an administrative procedure – as opposed to a binding arbitration – parties retain the right to take a case to the national court system.

Summary: To put these issues in context, several of the basic features of the UDRP must be re-emphasized. First, the UDRP establishes an international forum in which parties around the world now have equal and improved access to an inexpensive dispute settlement mechanism for resolving their domain name disputes. The scope of the UDRP is narrowly circumscribed to those cases brought by a party that can demonstrate the required three elements:

- That the domain name is identical or confusingly similar to a trademark in which that party has rights;
- That the domain name registrant has no rights or legitimate interests in the domain name; and
- That the domain name has been registered and is being used in bad faith.¹¹⁰

Each of these elements, as noted, must be proved by the complainant. The UDRP establishes a specialized set of procedures, tailored to the facts of a domain name dispute, and uses accredited dispute resolution service providers, who in turn draw from their rosters of expert neutrals to select panellists. The development of the facts and records for a case is based on a single submission from each of the parties, unless a panellist chooses to request additional information (and there is no guarantee that a panellist will exercise his or her discretion to do so). Furthermore, the scope of the remedies under the UDRP excludes monetary

damages and relates only to the status of the domain name registration. The complainant is normally required to cover the costs of the administrative procedure, unless the respondent has demanded a three-member panel, in which case the parties will share the extra costs of the panel. Finally, a complainant or domain name registrant is free to go to court either before or after the UDRP proceedings. If court proceedings are initiated within ten days of a UDRP decision, the status of the domain name in question will remain undisturbed (i.e. in the hands of the domain name registrant) until the completion of the court procedures.

Under these circumstances, it can be considered that the administrative system established by the UDRP survives the scrutiny of any due process concerns. The procedures and their implementation are appropriate to the nature of the disputes covered, and the degree of finality accorded to them. The UDRP also marks the first attempt to deal with cybersquatting in a systematic and internationally effective manner. Not surprisingly, therefore, the UDRP has received widespread attention. This is true for the legal and trademark community, and also for the general media.

The area of domain name disputes is but an early example of the emerging types of disputes that will arise as electronic commerce expands internationally. Linked through a series of contracts, all of the relevant players in the domain name system, including the technical company that enables access, have certain responsibilities under the dispute settlement procedure. Once a complainant chooses to join the procedure by submitting a complaint, the mechanics of the system are in place to guide the parties to a quick and fair result that will be automatically enforced. An administrative system such as the UDRP represents a pragmatic solution for disputes in the international marketplace of electronic commerce, avoiding the concerns and uncertainties associated with traditional litigation in national courts. This model can be used for dispute resolution in the ccTLDs, and can be of significant advantage to parties in developing countries.

2. Future legal issues for domain names

Intellectual property issues continue to receive attention in the DNS. The Final Report of the WIPO Internet Domain Name Process acknowledged that its recommendations targeted only the most serious problems caused by the conflict between domain

names and trademarks, and that other issues would require further consultation.¹¹¹ In July 2000, WIPO convened the Second WIPO Internet Domain Name Process to address domain name and intellectual property issues where continuing uncertainty remains, including recommendations on the bad faith, abusive, misleading or unfair use of:

- Personal names;
- International non-proprietary names (INNs) for pharmaceutical substances, of which there are more than 8,000;
- Names of international intergovernmental organizations (IGOs);
- Geographical indications, indications of source or geographical terms; and
- Trade names.

The Report of the Second WIPO Process, published in September 2001, found generally that the international legal framework for the protection of these identifiers is not as developed as that for the protection of trademarks. The Second Report was therefore more reserved in recommending international solutions. For example, in certain countries protection exists for geographical indications and trade names, but there is no international system applied in a relatively uniform manner. Moreover, with respect to personal names and the names of geographical localities, no clear protection exists when these terms are used outside commercial channels (and thus fail to qualify independently for trademark protection). The Second Report suggests that the international community still needs to decide whether it wishes to address these insufficiencies, in order to establish a legal basis for dealing with those practices that might be considered unacceptable.

The WIPO Second Report did recommend, however, that a mechanism be established to protect INNs against identical domain name registrations, and also that an administrative dispute-resolution procedure, similar to the UDRP, be established so that an IGO could bring a complaint when a domain name was creating a misleading association between the domain name registrant and the IGO in question. In this respect, it is possible for the Second WIPO Report – which also discusses the prospect of an international treaty – to have a significant impact. Developing countries can have input into these issues, as the Second

Report is still being considered by a committee of WIPO member States.

Finally, the Second WIPO Report also addresses a subject that is increasingly relevant today in view of the recent attention given to Internet privacy issues. It recommends that domain name registration companies in the existing and future gTLDs (e.g. .com, .net and .org as well as the newly approved gTLDs – .aero, .biz, .coop, .info, .museum, .name and .pro) should be required to provide accurate and publicly available WHOIS data about domain name registrants, subject to such users being clearly informed (and giving informed consent) about which data will be collected, the purposes for which it will be collected, and the uses to which it may be put, such as consumer protection, law enforcement and IP protection. Privacy issues inevitably arise when the details of a domain name registrant are sought even for legitimate purposes such as IP enforcement. A responsible approach to these issues, adopted by a ccTLD and made publicly available for inspection, can enhance confidence in national ccTLDs.

E. Concluding remarks and policy recommendations

The development of a national domain name system (DNS) infrastructure is an important means for enhancing the online exchange within developing countries, thus creating a valuable resource for communication, education and business. At the same time, however, domain names and the DNS give rise to a complex array of commercial, technical, policy and legal questions which typify many of the cross-border issues presented by the Internet and digital commerce. Developing countries need to understand these issues and formulate responses that are appropriate for the country's online community, satisfying relevant legal, cultural, economic, language and other dimensions. They should also promote public awareness and education about the DNS and the opportunities and benefits it offers.

Policy decisions are required in relation to the ccTLDs of developing countries, ones which foster not only a more relevant registration of domain names but also an overall confidence in the ccTLD space. The policies for ccTLDs should be carefully formulated, taking into account appropriate legal, cultural, economic and linguistic requirements. Developing countries' ccTLD administrators should improve domain name registration practices through clear agreements setting out the

rights and obligations of the parties, ensuring fairness to all eligible registrants requesting domain names, and establishing a clear policy for maintaining contact details of registrants, availability to third parties and privacy. Developing country ccTLD managers should become involved in the relevant forums available for exchanging information and participating in DNS policy-making.

It is recommended that developing countries also become involved in the ICANN reform process, as it provides a renewed opportunity to provide input about their perspectives, requirements and diversity, and to promote modalities for ICANN's work that better address the needs of their constituencies. Furthermore, they should consider establishing coopera-

tive relationships so as to increase their capacity to deal with and influence the current debate. In doing so, developing countries would take advantage of the work and progress in relation to domain names and intellectual property, including the establishment of dispute avoidance and dispute resolution policies.

Further to ICANN's adoption in 1999 of an international dispute resolution system, namely the Uniform Domain Name Dispute Resolution Policy (UDRP), it is also recommended that developing countries become more involved in the current UDRP debate and in the discussions about whether protection should be provided in the DNS for categories of identifiers other than trademarks, such as personal names, geographical indications and trade names.

Notes

- 1 See *E-Commerce and Development Report 2001*, at pp. 107-110.
- 2 The Anticybersquatting Consumer Protection Act, amending Section 43 of the Trademark Act of 1946, 15 U.S.C. §1125(d).
- 3 Complete information about ICANN is available through its website at www.icann.org and further discussion is provided below.
- 4 The Uniform Domain Name Dispute Resolution Policy is posted on ICANN's website at www.icann.org/udrp/. Further information and analysis concerning the UDRP are provided below.
- 5 Information concerning domain names and country domains in particular is available at the following websites:
 - Internet Corporation for Assigned Names and Numbers (ICANN): www.icann.org;
 - ICANN ccTLD information: www.icann.org/cctlds/;
 - International Telecommunication Union (ITU) Multilingual Domain Names: www.itu.int/mdns/resources/index.html;
 - World Intellectual Property Organization (WIPO) Domain Names information: <http://ecommerce.wipo.int/domains/index.html>;
 - Legal information concerning the Uniform Domain Name Dispute Resolution Policy: www.udrplaw.net/;
 - Activist observer group to ICANN at www.icannwatch.org/.
- 6 The International Telecommunication Union (ITU) located in Geneva, Switzerland, is an international organization within the United Nations system where Governments and the private sector coordinate global telecom networks and services. See the ITU website at www.itu.int.
- 7 The United States Government, acting through the Department of Commerce, has provided oversight of Internet and DNS developments, particularly when technical management issues were being dealt with by the Internet Assigned Numbers Authority (IANA). It has, for several years, been working as discussed below to transfer supervisory functions to ICANN.
- 8 "Noms de domain" in French and "nombres de dominio" in Spanish.
- 9 The term has started to appear in some but not all dictionaries. For example, *The American Heritage Dictionary of the English Language* (4th ed., Houghton Mifflin Company) provides the following definition: "A series of alphanumeric strings sepa-

rated by periods, such as *www.hmca.com*, that is an address of a computer network connection and that identifies the owner of the address". The Concise Oxford dictionary (10th ed., Oxford University Press) states that a "domain" is "a distinct subset of the Internet with addresses sharing a common suffix".

- 10 See the statistics maintained by NetNames International Ltd. at www.domainstats.com.
- 11 Mueller (2000a).
- 12 WIPO (1999, para.9).
- 13 See for example the statistics at www.zooknic.com/Domains/counts.html for the growth of *com/net/org/edu* domain names, and the statistics at www.denic.de/DENICdb/stats/domains_fancy.html for the growth of the German top-level domain ".de".
- 14 See Howe (1993-2001). For an even more technical definition, see the IANA website (www.iana.org/ipaddress/ip-addresses.htm) which states that "Internet Protocol (IP) addresses . . . are 32-bit numbers often expressed as 4 octets in "dotted decimal" notation (for example, 192.168.45.230)".
- 15 See note 11.
- 16 For a detailed publication on the history of the DNS, see Rader (2001).
- 17 He served as editor of an important series of more than 2,400 Requests for Comments (RFCs) from 7 April 1969 (the date of its inception) until his death in October 1998. RFCs are the definitions of the protocols and policies of the Internet, see Rader (2001).
- 18 See www.netsol.com. Verisign acquired Network Solutions Inc. (NSI), the operator of the .com, .net and .org gTLDs, in March 2000.
- 19 See ICANN, *ICP-3, A Unique, Authoritative Root for the DNS*, 9/7/01, at www.icann.org/icp/icp-3.htm.
- 20 See, for example, General Rules for the United Kingdom's .uk top-level and second-level domains at www.nic.uk/rules/rup2.html.
- 21 Of the 12 root servers that draw data directly from the "A" root server, seven currently are owned by the United States Government or operated by its contractors. For a more detailed analysis of who operates the root servers, see I Fromkin (2000).
- 22 See Diana Cabell, *Learning Cyberlaw in Cyberspace*, at www.cyberspacelaw.org/cabell/index.html.
- 23 See InterNIC FAQs at www.internic.net/faqs/authoritative-dns.html.
- 24 Among these new pseudo-TLDs are the *.ltd*, *.shop*, *.law*, *.love* and *.kids* domains, as well as *.web*. See, for example, www.new.net and www.web.net.
- 25 In practice, however, the United States Government reserves the *.gov* and *.mil* gTLDs for its exclusive use. The *.gov* TLD is operated by the United States General Services Administration. The *.mil* TLD is reserved exclusively for the United States military and is operated by the United States Department of Defense Network Information Center.
- 26 For example, the *.coop* gTLD opened its registration service on 31 January 2002. See www.cooperative.org/news/latest_news.asp?id=26. The operating entities for the *.pro* and *.aero* gTLDs are still not accepting registrations.
- 27 See www.iana.org/gtld/gtld.htm.
- 28 See www.neulevel.com/aboutnl/faqs.html.
- 29 As discussed below, developing countries may wish to sponsor a new multilingual TLD, particularly as the technology becomes available to make such internationalized TLDs a realistic possibility. See section B.2(c).
- 30 No new ccTLD will be accepted into the common A-root system unless it appears on this list; see www.iana.org/cctld/cctld.htm. See also the website of the International Organization for Standardization, which describes how the list is updated regularly by the ISO Maintenance Agency, at www.iso.org/iso/en/prods-services/iso3166ma/index.html.
- 31 See W. W. Fisher and S. Mendrey, *Domain Names and Trademarks*, at <http://eon.law.harvard.edu/h2o/property/domain/main.html>.

- 32 See, for example, policies for Italy, Japan and the Republic of Korea; see Fisher and Mendrey.
- 33 See Nominet's web site at www.nominet.uk. The Nominet.UK rules are listed at www.nominet.org.uk/rules.html.
- 34 See www.iis.se/regulations.shtml.
- 35 Difficult questions sometimes arise concerning who should be the proper ccTLD administrator, or even whether a particular country code should be delegated. See the website of the Internet Assigned Numbers Authority (IANA), which contains reports on noteworthy delegation and redelegation matters. (www.iana.org/cctld/cctld.htm). See, for example, the report of considerations concerning the delegation of .ps for Palestine, at www.iana.org/reports/ps-report-22mar00.htm.
- 36 A copy of latest version of this agreement, dated 31 January 2002, is available at <http://www.icann.org/cctlds/>.
- 37 See section 1.7 of the Sponsorship Agreement.
- 38 See Attachment F to the Sponsorship Agreement.
- 39 See the website for DENIC eG at <http://www.denic.de>.
- 40 See Newsbytes, *Singapore plans competition in domain name registration*, at www.newsbytes.com/cgi-bin/udt/i..le?client.id=newsbytes&story.id=172137.
- 41 See Regulation (EC) No. 733/2002 of the European Parliament and of the Council on the Implementation of the .eu Top Level Domain, 22 April 2002. *Official Journal of the European Communities*, L113/1 (30 April 2002).
- 42 The e-Europe initiative was endorsed by the European Council at its meeting in Lisbon in March 2000.
- 43 Regulation (EC) No. 733/2002, at Preamble.
- 44 Id.
- 45 See "Best Practice Guidelines for ccTLD Managers", 10 March 2001, at www.icann.org/cctlds/cctldconst-4th-best-practices-10mar01.htm.
- 46 See the "WIPO ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes", at <http://ecommerce.wipo.int/domains/cctlds/bestpractices/bestpractices.html>.
- 47 See the 'WIPO Ecommerce ccTLD Database' at <http://ecommerce.wipo.int/databases/cctld/output.html>.
- 48 See African Top Level Domains (AFTLD) Project at www.aftld.org/.
- 49 See, for example, the ICANN ccTLD web page at www.icann.org/cctlds/.
- 50 Despite the Internet's origins in the United States, it is currently estimated that by 2003 two thirds of all Internet users will be non-native English speakers. See "WIPO Briefing Paper: Internationalized Domain Names – Intellectual Property Considerations" at <http://ecommerce.wipo.int/domains/international/pdf/paper.pdf>; see also www.walid.com/en/docs/index.shtml.
- 51 ASCII is the American Standard Code for Information Interchange, and is the most prevalent format for text files used in computers networks. In an ASCII file, each alphabetical, numerical or special character is represented with a 7-bit binary number (a string of seven 0s or 1s). See Joint ITU/WIPO Symposium on Multilingual Domain Names at www.itu.int/itu-news/issue/2002/01/joint.html.
- 52 As noted in the WIPO Briefing Paper, (see note 50), DNS mapping technology has functioned thus far using only Latin characters that are used to write in a number of languages, including English, French, German, Italian and Spanish.
- 53 On 20 June 2001, VeriSign (previously Network Solutions), the operator of the .com registry, announced that it would provide full functionality for the registration of internationalized domain names for nearly 80 per cent of the world's Internet users. VeriSign has since introduced an Internationalized Domain Name Testbed, which allows users to register domain names in any script supported by Unicode. In November 2000, a company known as Walid introduced technology enabling the registration of domain names using the Hindi language. With this technology, Hindi speakers will be able to register Internet domain names using Hindi characters, and users will be able to access WorldWide Web content using those Hindi-language domain names. A resource page addressing IDNs, including a list of IDN solution providers, is maintained by the ITU at www.itu.int/mdns/resources/index.html.

- 54 See www.ietf.org. A working group within the IETF has the objective of specifying the requirements for internationalized access to domain names and formulating a standards track protocol based on those requirements.
- 55 The Discussion Paper states that “as part of its charter, the ICANN IDN Committee is tasked with anticipating the policy issues that would arise if and when ICANN confronts demonstrably deployable non-ASCII TLDs”.
- 56 See ICANN website for IDN Committee, at www.icann.org/committees/idn/.
- 57 See ICANN IDN Committee Discussion Paper on Non-ASCII Top-Level Domain Policy Issues at <http://www.icann.org/committees/idn/non-ascii-tld-paper.htm>.
- 58 Statistics provided by Walid, Inc. at www.walid.com (November 2001).
- 59 These registrars are located in many countries, such as Australia, Barbados, France, India, Italy, Japan, Jordan, Kuwait, New Zealand, Norway, Philippines, the Republic of Korea, Spain and Switzerland.
- 60 See the ICANN website for a listing of accredited registrars, at www.icann.org/registrars/accredited-list.html.
- 61 WIPO (2001b).
- 62 See ICANN website concerning DNS background and competition for domain name registration, at www.icann.org/general/background.htm#4.
- 63 See ICANN’s Instructions for Completing Shared Registry System Registrar Accreditation Application, at <http://www.icann.org/registrars/instructions.htm>. For example, to prepare an application, the applicant will need to collect the company’s financial information, including bank statements and insurance certificates, if available; audited annual reports if you are a publicly traded company; or other documents to demonstrate that the business has adequate working capital and commercial general liability insurance. With respect to technical information, the applicant will be required to describe current (or proposed) technical capabilities to provide SLD registration services, electronic back-up of registration data from customers, security for all registration information and continued SLD name use for SLD holders in the event the company goes out of business or ceases to operate as an accredited registrar.
- 64 A copy of the RRA is available at www.verisign-grs.com/registrar/dotcom/forms/rras.pdf.
- 65 The minimum payment security must be equal to at least the number of anticipated monthly registrations, multiplied by the number of years (minimum one year and maximum of ten years) and by the \$6 registration fee. The amount of the payment security will depend upon the registrar’s business plan, and a registrar may be required to increase the payment security if registration levels are consistently above the level covered by the current payment security. One further requirement linked with monetary issues is the so-called Security Instrument. This is a financial guarantee that would be employed by the registry if faced with a third-party claim in which the registrar did not indemnify VeriSign, as required by the RRA. The Surety Instrument must be for in the amount of \$100,000.
- 66 Up-to-date information concerning the domain name market is available from Zooknic Internet Intelligence at www.zooknic.com.
- 67 A “defensive registration” is a registration made by a user, often a trademark owner, who has no intention of using the registered name – perhaps because the user already has its own primary dotcom domain name – but nonetheless registers it to prevent others from taking it.
- 68 See “Analysts worried about VeriSign’s domain biz” CNET (June 3, 2002) at <http://news.cnet.com/investor/news/news-item/0-9900-1028-19995061-0.html?tag=ats>, referring to a monthly report of SnapNames.com, in which Verisign’s database declined by more than 900,000 names in April 2002 alone.
- 69 All numbers are drawn from Annex B, in which 61 ICANN-accredited registrars are compared regarding their end price for the registration of a .com domain name for one year; see also *Online Domain Generators: Market Research Report* at <http://domaingenerator.s5.com/report.htm>. The sum of \$35 was the price originally set that VeriSign could charge under its Cooperative Agreement with the National Science Foundation and later with the United States Commerce Department.
- 70 There are a number of companies that offer “domain name appraisal” services. See Lee Hodgson, *Domain Appraising – The Domain Name Fair Value Game*, at <http://ecommercebase.com/printTemplate.php?aid=266>.
- 71 ICANN is actually a registered non-profit corporation established in the United States under California law. The idea was that a private sector body would be more like the Internet itself: more nimble and efficient, able to react promptly to a rapidly changing environment, and, at the same time, open to meaningful participation by stakeholders developing policies

through bottom-up consensus. See *President's Report: ICANN – The Case for Reform*, 24 February 2002, at www.icann.org/general/lynn-reform-proposal-24feb02.htm.

- 72 Information about the GAC is available at www.icann.org/committees/gac/.
- 73 See ICANN Fact Sheet at www.icann.org/general/fact-sheet.htm.
- 74 ICANN's 19-member volunteer Board of Directors, has been constituted from a set of specialized technical and policy advisory groups, and through open, worldwide online elections.
- 75 See details about the Sponsorship Agreements for Japan and Australia at www.icann.org/cctlds/.
- 76 See the web page for the World Wide Alliance of Top Level Domains, ccTLD Constituency of the DNSO, at www.wwtld.org/. The Communiqués and Position Statements listed at www.wwtld.org/communiqué/ provide a review of the interactions between ccTLDs and ICANN.
- 77 See web pages on the ICANN site for the Committee on ICANN Evolution and Reform, at www.icann.org/committees/evol-reform/links.htm.
- 78 See *World eBusiness Law Report* (2002).
- 79 See *Miami Herald*, International Edition, 24 June 2002, p. 3B.
- 80 The Committee on ICANN's Evolution and Reform has published the "Recommendations for the Evolution and Reform of ICANN" available at www.icann.org/committees/evol-reform/recommendations-31may02.htm.
- 81 See ICANN's website pages devoted to the ERC at www.icann.org/committees/evol-reform/links.htm.
- 82 See WIPO website at <http://ecommerce.wipo.int>.
- 83 See, for example, Afiliats Sunrise Period and Challenge Procedure at www.afiliats.info/register/dispute_resolution/sunrise_challenge_overview.
- 84 The First WIPO Report, at paragraph 47, noted that many commentators in the WIPO Domain Name Process suggested that "the starting point should be the avoidance, rather than the resolution, of conflicts".
- 85 See a copy of Decision D1999-0001 at <http://arbitr.wipo.int/domains/cases/1999/d0000-0199.html>.
- 86 See ICANN's website for information about the UDRP, at www.icann.org/udrp/.
- 87 See the website of the Asian Domain Name Dispute Resolution Centre at www.adndrc.org/adndrc/index.html. ADNDRC is a joint venture between the Hong Kong International Arbitration Centre and the China International Economic and Trade Arbitration Commission.
- 88 See the website of CPR Institute for Dispute Resolution at www.cpradr.org/ICANN_Menu.htm.
- 89 See the website of the the National Arbitration Forum at www.arbforum.com/domains/.
- 90 See the website of the World Intellectual Property Organization at <http://arbitr.wipo.int/domains/>.
- 91 See UDRP, para. 4.a, at www.icann.org/udrp/udrp-policy-24oct99.htm.
- 92 See ICANN Policy, section 4(a)(i)(ii)and(iii), at www.icann.org/dndr/udrp/policy.htm.
- 93 *Ibid.*, section 4(b).
- 94 *Ibid.*, section 4(c) (i)-(iii).
- 95 *Ibid.*, section 5(iv).
- 96 *Ibid.*, section 6(b).
- 97 *Ibid.*, section 5(c). If the complainant requests a single-member panel and the respondent does not object, the provider alone assigns a single panellist from its roster to the case. *Ibid.*, section 6(e). If a three-member panel is selected, one panellist is selected from the list of candidates provided by the complainant and the respondent. The third panellist is appointed by the provider from a list of five candidates submitted by the provider to the parties, the selection from among

the five being “made in a manner that reasonably balances the preferences of both Parties”. Ibid., section 4(b) (iv). The typical approach is to allow each party to strike out up to two names from the list of five.

98 Ibid., section 4(a).

99 Ibid., section 5(a).

100 Ibid., section 5(e).

101 Id., para. 4.i.

102 The procedure also has a high rate of settlement; agreements between the parties have been reached in approximately 20 per cent of the filed cases.

103 See Geist (2001); Mueller (2001b); Stewart (2001).

104 WIPO and NAF attract the largest number of complaints and e-Resolutions attracted the lowest share of cases. Despite the highest fees, as of July 2001, WIPO had 58 per cent of the UDRP caseload as compared with 34 per cent for NAF and only 7 per cent for eResolution.

105 Kur (2001).

106 Id., at p 72

107 Donahey (2001).

108 Ibid.

109 See UDRP Rules, section 5(d).

110 See UDRP, para. 4.a.

111 See WIPO Final Report, Executive Summary.

References and bibliography

- Donahey M (2001), *The UDRP – Fundamentally Fair, But Far From Perfect* (online at www.dnso.org/clubpublic/nc-udrp/Arc00/doc00002.doc).
- Froomkin, M. (2000) *Wrong Turn in Cyberspace*, at <http://personal.law.miami.edu/~froomkin/articles/icann-main.htm>.
- Geist M (2001), *Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, online at <http://aix1.uottawa.ca/~geist/geistudrp.pdf>
- Howe D (1993-2001) *The Free On-line Dictionary of Computing*
- Joint ITU/WIPO Symposium on Multilingual Domain Names, at <http://www.itu.int/itunews/issue/2002/01/joint.html>.
- Kur A (2001), *A Study by the Max-Planck Institute for Foreign and International Patent, Copyright and Competition Law*, in cooperation with the Institute for Intellectual Property Law and Market Law, University of Stockholm, and the Institute for Information Law, Technical University of Karlsruhe.
- Mueller M (2000a) 'Technology and Institutional Innovation: Internet Domain Names', *International Journal of Communications Law and Policy* 5, Summer, at http://www.ijclp.org/5_2000/ijclp_webdoc_1_5_2000.html.
- Mueller M (2000b), *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy* <http://dcc.syr.edu/roughjustice.htm>
- Rader RW (2001), *The History of the DNS*, at www.whmag.com/content/0601/dns.

Regulation (EC) No. 733/2002 of the European Parliament and of the Council on the Implementation of the .eu Top Level Domain, 22 April 2002. *Official Journal of the European Communities* L113/1 (30 April 2002).

Stewart IL (2001). 'The Best Laid Plans: How Unrestrained Arbitration Decisions Have Corrupted the UDRP', *Federal Communications Law Journal*, vol. 53, April , pp. 511-532.

"WIPO (2001) ccTLD Best Practices the Prevention and Resolution of Intellectual Property Disputes", at <http://ecommerce.wipo.int/domains/cctlds/bestpractices/bestpractices.html>.

WIPO (2001a) Briefing Paper: Internationalized Domain Names – Intellectual Property Considerations, at <http://ecommerce.wipo.int/domains/international/pdf/paper.pdf>; see also <http://www.walid.com/en/docs/index.shtml>.

WIPO (1999). *The Management of Internet Names and Addresses, Final Report of the WIPO Internet Domain Name Process*, at <http://wipo2.wipo.int/process1/report/finalreport.html#II>

WIPO (2001b), *The Recognition of Rights and the Use of Names in the Internet Domain Name System, Report of the Second WIPO Internet Domain Name Process*, at <http://wipo2.wipo.int/process2/report/pdf/report.pdf>

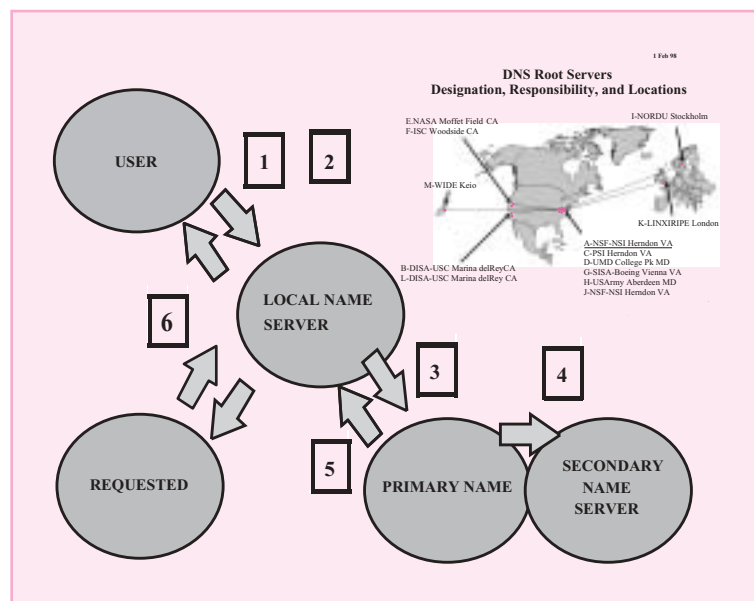
ANNEX I

Overview of the DNS

This annex describes the basic method by which a domain name functions to direct users to a specific web site. For purposes of illustration, reference is made to the common situation, in which a user seeks to access a site on the World Wide Web (www) using the Internet browser on the user's computer.

1. After the domain name is typed into the respective input field, the first step is that the browser will send a request to a local nameserver to "resolve" the IP address of the specified web site. The local nameserver is therefore also called a DNS resolver. They are located strategically with Internet Service Providers (ISPs) or in other institutional networks.
2. As a second step, the DNS resolver will issue a request to a "root" domain nameserver, which will return the IP address of the primary and secondary nameservers responsible for the TLD (e.g., .com) of the requested web-site.
3. The DNS resolver will then contact the primary server of that TLD, where the IP address information is held in a database, and the primary server would satisfy the request from the DNS resolver.

Chart 6
DNS Resolving



4. In case the primary nameserver would not be available, the DNS resolver would contact the secondary nameserver which would also hold the corresponding information.
5. In either case, the DNS resolver would return to the user's browser with the IP address for the requested domain.
6. Using that IP address, the browser would then contact directly the requested web site and, finally, the web site information would be sent to the DNS resolver and could be accessed by the user.

This process can often be performed while skipping some of the steps listed above. DNS resolvers routinely download and copy (or cache) the information contained in the root servers. They also store for a period the IP addresses that have been resolved recently. Using this cache, the DNS resolver is often able to satisfy the request without contacting the root server. In fact, the cache function is essential on the Internet for reasons of performance. The root servers could not properly handle billions of requests a day and, if they were required to do so, it

ANNEX II

Registrar Prices for Domain Name Registration Status as of 15/06/02

Source concerning information Registrar/Country/URL:

<http://www.icann.org/registrars/accredited-list.html>

LEGEND:

*: two year minimum registration

**: two domain registrations minimum

35(35): 35 = prices 15/06/02; (35) = price September/October 2001

URL: URL could not be accessed on the date of last visit (15/06/02)

not yet: registrar does not yet offer registration services (15/06/02)

no rg-s: registrar does not offer "pure" registration services, mainly because company only offers "package" services which include domain name registration services

wsale: wholesale only

lang.: no information because web side is run in language other than English/French/Spanish

hosting: registrar only offers hosting services, no "pure" registration services

.info/.pro:registrar only offers registration services for these TLDs, not for .com domain

members:members only; need to lock in

all prices are the prices for one year and also of the first year of registration

all USD prices are approx. (< 10 USD the exact prices are listed)

all web-sides last visited on 15/06/02

no special offers are listed

Registrar Prices for Domain Name Registration (.com only)				
Registrar	Country	appr. US\$ domain/year ¹	URL	
! AholaNIC LLC	United States	17*	www.alohanic.com	
#1 Domain Names International, Inc. dba 1 dni.com	United States	URL(35)	www.1dni.com	
@Com Technology LLC	United States	not yet	www.AtComTechnology.com	
007Names, Inc.	United States	15	www.007names.com	
1 eNameCo	United States	17(17)	www.eNameCo.com	
123 Easy Domain Names, Inc. dba Signature Domains	United States	35(15)	www.signatredomains.com	
123 Registration, Inc. d/b/a 123registration.com	United States	35(35)	www.123registration.com	
1stDomain.Net, a division of G+D International LLC	United States	25*(25)	www.1stdomain.net	
2Day Internet Limited dba 2day.com	New Zealand	not yet	registrar.2day.com	
A Technology Company, Inc. dba namesystem.com	Canada	12(15)	www.namesystem.com	
AAQ.COM, Inc.	United States	.info	www.aaq.com	
Abacus America, Inc. d/b/a Name4ever	United States	20(20)	www.names4ever.com	
ABR Products Inc. dba Nitin Networks	United States	35	names.nitin.com	
Abu-Ghazaleh Intellectual Property (AGIP)	Jordan	no rg-s	www.agip.com	
Active ISP ASA	Norway	35	www.activeisp.com	
Address Creation	United States	15(15)	www.addresscreation.com	
Adgrafix Corporation	United States	15	www.adgrafix.com	
Alice's Registry, Inc.	United States	35(35)	www.ar.com	
All West Communications, Inc. DBA AWRegistry	United States	35(35)	www.awregistry.com	
Alldomains.com	United States	35(35)	www.alldomains.com	
America Online, Inc.	United States	no rg-s	www.aol.com	
Amercian Domain Name Registry	United States	-		
Antelecom, Inc.	United States	20	www.antelecom.net	
Arsys Internet, S.L. dba soloregistros.com	Spain	30	www.soloregistros.com	
Ascio Technologies, Inc.	Denmark	no rg-s	www.ascio.com	
BB Online UK Limited	United Kingdom	18(18)	www.nominate.net	
Blueberry Hill Communications, Inc. d/b/a 4Domains.com	United States	25	www.4domains.com	
BrookMyName SAS (formerly Worldnet)	France	30	www.bookmyname.com	
British Telecommunications (BT plc)	England	no rg-s	www.bt.com	
BulkRegister.com	United States	wsale.	www.bulkregister.com	
C I Host, Inc.	United States	URL	www.cihost.com	
Capital Networks Pty Ltd.	Australia	20(20)	www.totalnic.net	
CASDNS, Inc.	United States	25	www.CASDNS.net	
Catalog.com	United States	35(35)	www.catalog.com	
Centergate Research Group, LLC	United States	no rg-s	www.centergate.com	
Central Registrar dba Domainmonger.com	United States	17	www.domainmonger.com	
Computer Data Networks dba Shop4domain.com and Netonedomains.com	Kuwait	22(20)	www.shop4domain.com	
CORE Internet Council of Registrars	Switzerland	no rg-s	www.corenic.org	
Corporate Domains, Inc.	United States	.info	www.corporatedomains.com	
Cronon AG Berlin, Niederlassung Regensburg	Germany	wsale.	www.cronon.org	
CSL Computer Service Langenbach GmbH d/ b/a joker.com	Germany	12(24)	www.joker.com	
Cyidian Technologies	United States	15	www.Cyidian.com	
Deutsche Telekom AG	Germany	no rg-s	www.dtag.de/katalog-online/domain	

¹ prices listed in brackets indicate the price Sep/Oct 01.

Registrar	Country	appr. US\$ domain/year ¹	URL
DevelopersNetwork.com., Inc. dba DomainInvestigator.com	Canada	15	www.DomainInvestigator.com
Direct Information Pvt Ltd d/b/a Directi.com	India	8.50	www.directidomains.com
Dodora Unified Communications, Inc.	United States	no rg-s	www.dodora.net
Domain Bank, Inc.	United States	35(35)	www.domainbank.com
Domain Intellect Pty Ltd.	Australia	no rg-s	www.domainintellect.com
Domain Registration Service, Inc. dba dotEarth.com	United States	12*(10)	www.dotEarth.com
Domain The Net Technologies Ltd.	Israel	lang.	www.DomainTheNet.com
Domaininfo AB, aka domaininfo.com	Sweden	25*(25)	www.domaininfo.com
Domain-It!, Inc. dba Domain-It!	United States	35*	www.domainit.com
DomainName, Inc.	United States	30	DomainName.com
DomainPeople, Inc.	Canada	35(35)	www.domainpeople.com
DomainPro, Inc.	United States	.pro	www.domainpro.com
DomainProcessor.com, a division of Funpeas Media Ventures, LLC	United States	20	www.DomainProcessor.com
DomainRegistry.com.Inc.	United States	30(30)	www.DomainRegistry.com
DomainSite.com, Inc.	United States	13(13)	www.domainsite.com
DomainZoo.com, Inc.	United States	20(20)	www.domainzoo.com
DomReg Ltd. dba ATLNTD.com	Russia	lang.	www.atlntd.com
Dotster, Inc.	United States	15(15)	www.dotster.com
Eastern Communications Company Limited	China	URL	www.reg.eastcom.com
Easyspace Limited	United Kingdom	25(17)	www.easyspace.com
Echo, Inc.	Korea	lang.	www.domainrg.com
eMarkmonitor Inc. dba Markmonitor	United States	wsale	www.markmonitor.com
eNom, Inc.	United States	30(30)	www.enom.com
EPAG Enter-Price Multimedia AG	Germany	18*(25)	www.epag.de
Equitron Inc. d/b/a DomainNameRegistration.com	United States	35*	www.domainnameregistration.com
ExtremeNames.com	United States	URL	www.extremenames.com
Gabia, Inc.	Korea	lang.	www.name7.com
Gal Communication (CommuniGal) Ltd.	Israel	13	www.galcomm.com
Gandi SARL	France	URL(12)	www.gandi.net
GKG.NET, INC. (Formerly GK Group L.L.C.)	United States	9.99(10)	www.gkg.net
Global Media Online Inc. d/b/a Discount-Domain.com and Onamae.com	Japan	lang.(35)	www.interg.or.jp
GlobalHosting, Inc. d/b/a SiteRegister	United States	not yet	www.siteregister.com
Globedom Datenkommunikations GmbH, d/b/a Globedom	Austria	wsale.	www.globedom.com
Go Daddy Software, Inc.	United States	8.95(9)	www.godaddy.com
Future Media Network	Japan	lang.	www.fm-net.ne.jp
HANGANG Systems, Inc. dba Doregi.com	Korea	14	www.doregi.com
HiChina Web Solutions Limited	China	URL	www.net.cn
Hosting-Network, Inc.	United States	not yet	www.hosting.network.com
I.D.R Internet Domain Registry LTD.	Israel	12	www.idregister.org
iHoldings.com, Inc. d/b/a DotRegistrar.com	United States	15**(14)	www.DotRegistrar.com
IKANO Communications, Inc.	United States	no rg-s	www.ikano.com
INAMES Corp.	Korea	URL	www.i-names.co.kr
InnerWise, Inc. d/b/a ItsYourDomain.com	United States	15(15)	www.itsyourdomain.com
InterAccess Co.	United States	-	now www.hosting.com
Interactive Telecom Network, Inc.	United States	not yet	ww.domaindomain.com
Intercosmos Media Group, Inc.	United States	15(15)	www.directnic.com

Registrar	Country	appr. US\$ domain/year ¹	URL
Interdomain S.A.	Spain	30	www.interdomain.org
Internet Domain Registrars d/b/a Registrars.com	Canada	-(35)	now www.verisign.com
Internetplaza City Co., Ltd	Korea	lang.	www.inplaza.net
Internetters Limited	United Kingdom	34*	www.internetters.com
Key-Systems GmbH d/b/a domaindiscount24.com	Germany	12(12)	www.domaindiscount24.com
Korea Information Certificate Authority, Inc. dba DomainCA.com	Korea	no rg-s	www.domainca.com
Marksonline, Inc.	United States	no rg-s	www.marksonline.com
Melbourne IT Ltd trading as Internet Names Worldwide	Australia	35(35)	www.melbourneit.com
Mobilcom City Line d/b/a topnet AG	Germany	no rg-s	www.topnet.de
Mr. DomReg.com Inc.	Canada	25(25)	www.mrdomreg.com
Namebay	Monaco	12(12)	www.namebay.com
NameEngine, Inc.	United States	no rg-s	www.nameengine.com
NameScout Corp.	Barbados	25*	www.namescout.com
Namesdirect.com, Inc.	United States	30(30)	www.namesdirect.com
Namesecure.com, Inc.	United States	15(35)	www.namesecure.com
Namezero.com, Inc.	United States	20	www.namezero.com
Net Searchers International Limited	United Kingdom	no rg-s	www.netsearchers.com
NetBenefit plc aka NetNames	United Kingdom	49*(35)	www.netnames.co.uk
Netblue Communications Co., Ltd.	Korea	lang.	www.domainshock.com
Neteka Inc. dba namesbeyond.com	Canada	18	www.namesbeyond.com
Netpia.com, Inc.	Korea	lang.	www.ibi.net
Network Solutions, Inc. Registrar	United States	35(35)	www.networksolutions.com
New Dream Network, LLC dba Domainitron.com	United States	25	www.domainitron.com
Nominalia Internet S.L.	Spain	34(37)	www.nominalia.com
Nordnet	France	35	www.nordnet.net
Omnis Network, LLC	United States	15(20)	www.omnis.com
OnlineNIC, Inc.	United States	wsale.	www.onlinenic.com
OVH	France	8.90	www.ovh.com
pair Networks, Inc. d/b/a pairNIC	United States	19	www.pair.com
Parava Networks, Inc. d/b/a RegistrareYa.com and nAAME.com	United States	35(35)	www.parava.net
pAsia, Inc.	Taiwan	lang.	www.pasia.com
Philippines Registry.Com, Inc.	Philippines	35*	www.Philippineregistry.com
Polar Software Limited d/b/a signdomains.com	India	9.95	www.signdomains.com
Primus Telecommunications Pty Ltd trading as PlanetDomain and PrimusDomain	Australia	15(35)	www.planetdomain.com
PSI Japan	Japan	15(67)	www.psi-domains.com
PSI-USA, Inc.	United States	no rg-s	www.psi-usa.com
R & K Global Business Services d/b/a 000Domains.com	United States	14	www.000domains.com
Register.com, Inc.	United States	35(35)	www.register.com
REGISTER.IT SPA	Italy	35	we.register.it
RegistrarsAsia Pty Ltd	Australia	39	www.registrarsasia.com
Registration Technologies, Inc.	United States	15	www.RegistrationTek.com
Research Institute for Computer Science, Inc.	Japan	lang.	www.rics.co.jp
SafeNames Ltd.	United Kingdom	35	www.safenames.net
Schlund+Partner AG	Germany	hosting	www.schlund.de
Secura GmbH	Germany	30(60)	www.domainregistry.de
Shaver Communications, Inc.	United States	no rg-s	www.web2010.com
SiteName Ltd.	Israel	13	www.sitename.com

Registrar	Country	appr. US\$ domain/ year ¹	URL
Stargate Communications, Inc.	United States	14(16)	www.stargateinc.com
Talk.com, Inc.	United States	no rg-s	www.talk.com
The NameIT Corporation d/b/a AITdomains.com	United States	19(19)	www.aitdomains.com
The Registry at Info Avenue d/b/a IA Registry	United States	13(15)	www.IARegistry.com
TierraNet Inc. DBA DomainDiscover	United States	25*(25)	www.domaindiscover.com
TLDs Inc. d/b/a SRSplus	United States	wsale.	www.srsplus.com
Today and Tomorrow Co., Ltd.	Korea	URL	www.tt.co.kr
Total Web Solutions Limited Trading as TotalRegistrations	England	12(12)	www.totalregistrations.com
Transpac	France	no rg-s	www.oleane.net
Triara.com S.A. de C.V.	Mexico	no rg-s	www.triara.com
Tucows Inc.	Canada	hosting	www.tucows.com
Tuonome.it.srl	Italy	15	www.tuonome.it
Universal Registration Services, Inc. dba NewDentity.com	United States	members	www.newdentity.com
USA Webhost	United States	15	www.usawebhost.com
Venture.com Inc. dba DomainCity.com	Korea	not yet	www.domaincity.com
Virtual Internet Plc.	United Kingdom	15(25)	www.vi.net
Wild West Domains, Inc.	United States	not yet	www.wildwestdomains.com
Wooho T & C Ltd., d/b/a rgnames.com	Korea	lang.	www.rgnames.com
Xin Net Corp., Ltd.	China	lang,	www.chinadns.com
Yesnic Co., Ltd.	Korea	18(18)	www.yesnic.com