Industrie Canada

IC

Domain Name System Reform and Related Internet Governance Issues

A Consultation Paper

Prepared by Industry Canada

with the assistance of
Omnia Communications Inc.

0 96809 24053 2

August 1998

Canada

Industry Canada Industrie Canada

Domain Name System Reform and Related Internet Governance Issues

A Consultation Paper

Prepared by Industry Canada

with the assistance of
Omnia Communications Inc.

August 1998

Canada

This publication is also available electronically on the World Wide Web at the following address:
http://e-com.ic.gc.ca/english/documents/dns_intro.html

This document can be made available in alternative formats for persons with disabilities upon request.

Additional printed copies of this publication are available from:

Distribution Services
Communications Branch
Industry Canada
Room 205D, West Tower
235 Queen Street
Ottawa, ON K1A 0H5
Tel.: (613) 947-7466
Fax: (613) 954-6436

Comments may be sent by e-mail to the following address:
dns.consultation@e-com.ic.gc.ca

Comments can also be sent by fax to the attention of "DNS Consultation" at (613) 941-1164.

Submissions must be received on or before September 8, 1998.

Cat. No. C2-358/1998 E
ISBN 0-662-27128-9
52015E

Aussi disponible en français sous le titre *Réforme du système des noms de domaine et examen de questions connexes sur la gestion d'Internet: Document de consultation.*
http://e-com.ic.gc.ca/francais/documents/dns_intro.html

Domain Name System Reform and Related Internet Governance Issues

TABLE OF CONTENTS

1. THE INTERNET, THE DNS & ELECTRONIC COMMERCE

The global network of networks known as the Internet is rapidly becoming an important element of economic growth in Canada and the world's other developed countries. It has given rise to an economic activity that was almost unheard of five years ago — electronic commerce (or "e-commerce"), the buying and selling of goods and services online. Some research firms predict that the global value of e-commerce, including both business-to-business and consumer transactions, will reach between US$300 and 400 billion by 2002. This represents roughly a doubling of activity every year from 1997 onward.

As telecommunications networks and information technology become more pervasive and influential in everyday life, electronic commerce holds the potential to make Canada more competitive in the global economy, create entrepreneurial opportunities and jobs, and stimulate innovation. The ultimate promise of this new commercial marketplace is an unprecedented level of efficiency, choice, convenience and prosperity, for business people and consumers alike — if the right decisions are taken about how to fulfill this promise.

A role as major engine of the economy is an improbable one for the Internet, given its historical roots. For two decades, the Internet played a crucial but relatively obscure part in a highly specialized field of government-sponsored communications research. From its early beginnings as the ARPANET, it performed two general functions. First, it was a testbed for advanced research on networking technologies, including packet switching, which was later to find widespread applications in telecommunications. Second, it was a communications vehicle for a family of research scientists, academics, defence contractors and government officials who needed a convenient and secure way to share information and databases about their work. That work developed into a way of sending messages across different networks — "internetworking" — that became known as the Internet protocols, or IP.

The Internet grew through the 1970s and 1980s as other specialized users, including Canadian computer scientists, realized the potential for this technology and worked to link more and more networks to the original ARPANET. The power of the technology lay

in the fact that it operated on an "open" standard — a publicly available, non-proprietary software platform that could send information between different kinds of computers, operating systems and network links. It became a computer lingua franca that today links approximately 100,000 public and private networks around the world. It proved to be highly adaptable not only to expansion but also to the introduction of new functions, which can be layered on to existing functions. Certainly the best known and most widely used "new" function or layer is the World Wide Web (the Web), the idea for which was first formulated in Geneva in 1989. It was the Web, and in particular the graphical Web browser, that more than any other single factor made the Internet a popular and commercial medium, and eventually led to the discussions on reform that are the subject of this paper.

The power, flexibility and dramatic growth of the Internet are the product of an unusual system of governance — a combination of top-down policy-making and financing by the U.S. government and bottom-up technical coordination by non-governmental, partly international bodies which are creatures of individual and professional initiative. This hybrid governance model, along with an uncanny capacity to absorb both innovation and new users, have created a popular image of the Internet as a chaotic and unruly forum without structure or leadership.

This is a misleading image, belying several important attributes of the Internet that have brought it to a watershed divide in 1998. The Internet was and still is sponsored by the U.S. government, and operates under the auspices of several federal agencies, including the Defense Information Systems Agency (DISA), the Defense Advanced Research Projects Agency (DARPA), and the National Science Foundation (NSF) — though most operational activities are coordinated by non-governmental bodies such as the Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), Internet Assigned Numbers Authority (IANA) and Regional Internet Registries (RIRs). Aside from the fact that most of the world's Internet user population and traffic is still American-based, the essential technical infrastructure for routing this traffic is highly centralized and also physically located in the United States. Although the Internet, and especially the Web, have moved a long way from their roots in specialized military and scientific research, the Internet is no less a marvel of engineering coordination, dependability and structural

intricacy — indeed more so today than ever before, given its ever-expanding size and functionality.

Importance of the DNS

One of the essential components of this complex global structure is designed to identify individual computers linked to the Internet — the Domain Name System, or DNS. Once a subject of little interest to anyone but the computer scientists who created and maintain it, the DNS has, for reasons explored throughout this paper, become both a source of international controversy and one of the keys to the future of electronic commerce.

The DNS is like a vast digital address book with two kinds of entries — one known as the "name space," the other as the "address space." The first is a set of millions of names — like ic.gc.ca and www.apple.com — which have become familiar not only to email and Web users, but to almost anyone who reads newspapers and billboards or watches TV. The other is a less familiar set of numbers in the form of four-part strings of up to 12 digits separated by dots, like 111.222.333.444. These IP (Internet protocol) numbers are the unique addresses that are assigned to every computer connected to the Internet. The job of the DNS is to map or match the names that appear in Web browsers and email headers to the IP numbers that identify the ultimate destination of a transmission — an email to the office or request for product information from a Web site.

Domain names are organized in a hierarchy, starting with the "root" or most basic level. Actual domain names include what is called a "top level domain" or TLD, which appears as the suffix at the right-hand end of the name. There are two kinds of TLDs: *generic top level domains* or gTLDs, like ".com" and national top level domains or *country codes*, like ".ca" for Canada, referred to as ccTLDs. Domain names become usable for individual addressing purposes at the next level down in the hierarchy — that of the second level domains or SLDs. These take the form of "mybusiness.com" or "mybusiness.ca" and can be extended to a third level and beyond to identify subsets or divisions of the addressee's domain.

The DNS covers over 200 national TLDs, which are used to some degree throughout the world — except in the United States, where the .us designation has been almost completely eclipsed by a preference for the generics, above all the .com domain, the most popular and widely recognized of all the generics. A set of seven generic TLDs was created originally to indicate the function of the space, and users, involved: .com for commercial users, .org for not-for-profit organizations, .net for network service providers, .gov for government agencies, .mil for military users and networks, .edu for educational institutions and .int for international agencies.

There are analogies between the DNS and the international postal and telephone systems. In order for all these systems to work, recipients must have unique addresses that are known or available to other users, and messages must be addressed in such a way that they routinely find their intended recipient, without ambiguity or duplication. Not unlike the DNS, the postal system tries to match the names of individuals, organizations and buildings to street addresses and postal codes, while the telephone system matches many of these same names to local numbers, area and country codes. Users of all these systems have come to expect them to be fast and unfailing.

The analogy can be extended to the realm of commercial activity. Just as the domestic and international exchange of goods and services could not function without stable, publicly available postal and telephone systems, neither can the Internet equivalent — electronic commerce — be expected to prosper without a stable international platform for the transmission of advertising and promotional messages, orders, payments, service and support information, and a host of "digitized" goods such as software, music, databases and other proprietary information like newspaper content.

The Challenges of Coordination

But the postal and telephone analogies only go so far, thanks to the unique organizational and technical aspects of the DNS.

First of all, as noted above, Internet policies and operations are largely controlled within the United States, with only incidental influence being exercised by other countries. This

is in sharp contrast to the postal and telephone systems, which are coordinated internationally, but regulated on a strictly national basis from country to country.

Moreover, despite the close mapping that must be maintained between the name and address spaces of the DNS, the management of each is handled by two very different bodies. While both operate separately from government under contract to public agencies, one is a for-profit corporation, Network Solutions, Inc. (NSI), the other a small group of academics which runs the Internet Assigned Numbers Authority (IANA), itself more a set of operating functions than an actual organization. Following approval by Congress of commercial activities on NSFNet in 1992, the U.S. government hired NSI to manage all registration and technical functions connected with the generic top level domains, including the ubiquitous .com domain. NSI performs these functions for commercial gain and does so on a monopoly basis sanctioned by its contract with the U.S. government. This contract expires on September 30, 1998.

The role of IANA, which is run by Dr Jon Postel and his colleagues at the University of Southern California, is to manage the address space of the DNS — which includes allocating large blocks of numerical IP addresses to three regional registries: the American Registry for Internet Numbers (ARIN: mainly North America); Réseaux IP Européens (RIPE: Europe); and Asia/Pacific Network Information Center (APNIC: Asia/Pacific). They in turn allocate smaller address blocks to major Internet service providers, which are subsequently sub-divided among smaller suppliers and eventually to end-users.

While NSI and IANA thus play the key roles in management of the DNS, many other coordinating functions are handled by the "bottom-up" non-government bodies alluded to earlier. One of the paradoxes of Internet governance is that, despite the dominant role played by the U.S. government, a principal policy goal of the U.S. authorities has been to encourage autonomous bodies to conduct research and development on networking technologies, as well as to take responsibility for most of the technical infrastructure of the Internet. These tasks have been handled by a number of different groups around the world, but the basic management of the Internet has devolved to a handful of

organizations, notably the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB) and the World Wide Web Consortium (W3C).

These groups act like quasi-official standards-setting bodies. While they are able to impose standards on the international Internet community, they do so with only indirect government sanction, using methods that would be considered unusual in other fields. They are open in their membership and reasonably democratic in their procedures, often operating on the so-called "rough consensus and running code" system, whereby technical proposals are carried if they do not meet serious opposition and someone can claim they have a related piece of the software code operational in the real world. Nevertheless, according to many interest groups, especially commercial and business interests, these technical groups are not representative of, or accountable to, users in any meaningful way.

The Impetus for Change

The DNS, and perhaps the Internet as a whole, have reached a turning point.

Over the last year, more and more calls for reform of the DNS have been heard, from end-user groups, governments, the coordinating bodies themselves and many other interested parties. While not always in the foreground of discussions, two main factors are responsible for this state of affairs: the unstoppable growth of the Internet and its transformation from an obscure scientific research project to a popular and commercial medium that already reaches an "audience" of well over 100 million people.

The commercialization of the Internet has taken place in several stages, beginning at least as far back as the mid-1980s and the launch of MCI Mail on the Internet, and continuing with approval from the U.S. Congress for commercial activities on NSFNet in 1992. One of the most important subsequent developments was the widespread introduction of the graphical Web browser known as Mosaic in the mid-1990s, which allowed users without specialized knowledge of computing to become part of what had previously been a small community comprised largely of academic researchers and scientists.

The many new members of the Internet "community" that have come online in the last couple of years include ordinary consumers, mainstream business people and, not least of all, users from countries other than the United States. These new user groups bring needs and values to the Internet that have little or no connection with the past. They have high expectations, yet little interest in either the technical underpinnings of the Internet or the unusual governance model that has prevailed for the last 25 years. And both new users and many traditionalists have frustrations with the way the DNS is governed and managed today.

Critics have expressed objections to the for-profit, monopoly arrangement enjoyed by NSI as the sole source of second-level domain names using .com and the other gTLDs. For some, this is an issue of public trust and concern for the general welfare of Internet user groups. Others have called for competition in the registration function and an end to the NSI monopoly because they feel they are being shut out of business opportunities in the sale and management of domain names.

Another widespread criticism concerns lack of accountability — not only on the part of the monopoly supplier of domain names, NSI, but on the part of the coordinating bodies as well. Many user groups, especially those involving newer commercial interests, do not feel they have any meaningful voice in the management of the DNS and governance issues in general. This desire for greater accountability has reinforced the argument, at least for some, that the system should be opened up to private-sector competition. The goal of greater accountability is being championed by many groups and individuals both inside and outside the United States.

Even though the DNS has, for the most part, functioned remarkably well over the years, there are concerns that the informal system maintained by IANA, with the support of the other major technical coordinating bodies, is ill-suited to a role as a global platform for electronic commerce, which is growing by leaps and bounds. This is not regarded as just a technical issue, but as a policy issue as well. The rapid commercialization of the Internet has changed the climate of opinion on the uses and value of domain names — and in particular on the issue of whether new gTLDs should be created, how many, at what pace and under whose control. SLDs have evolved from being regarded as convenient

mnemonics to branding and marketing devices with an often critical role to play in the Internet presence of commercial businesses and other organizations.

Finally, much of the pressure for reform of the DNS has developed because of conflicts between domain name holders and trade-mark owners who feel their legal rights are being infringed by the registration and use of certain names — and in the United States especially, the use in domain names of famous brands by persons allegedly not authorized to do so. Many parties have called for creation of a dispute resolution process to address these kinds of conflicts. Although the process might take a number of different forms, the objective is to minimize expensive resorts to litigation, as well as to ensure the continuing stability of the Internet.

The U.S. White Paper

After months of intensifying international debate, stakeholders around the world focussed their attention on a single document issued on June 5, 1998 by the United States Department of Commerce through the National Telecommunications and Information Administration (NTIA). Entitled simply "Management of Internet Names and Addresses" (Docket Number: 980212036-8146-02), this document is more commonly referred to as the "White Paper." It is technically speaking a Statement of Policy which does not have the force and effect of law.

Nevertheless, the White Paper is the Clinton Administration's definitive statement on reform of the DNS. It is the culmination of a study and consultative process that included publication last January of a draft policy statement on reform of the DNS referred to as the "Green Paper." This process was initiated a year ago, under the Clinton Administration's Framework for Global Electronic Commerce. As the opening passage of the White Paper states, "the President directed the Secretary of Commerce to privatize the domain name system (DNS) in a manner that increases competition and facilitates international participation in its management."

As the reader will see in the pages that follow, the White Paper has put forward a number of proposals for reform which are now the subject of intense discussion. The most far-

reaching of these proposals is the suggested creation of a private, not-for-profit body, referred to as the "new corporation," that would take over all the main policy, technical and governance functions of the DNS.

The Government of Canada has studied the White Paper closely and it is the subject of considerable analysis in this paper. The White Paper establishes a number of important principles for moving the reform process forward. At the same time, it leaves a number of important questions unanswered and raises concerns which the Canadian government will continue to follow in the months ahead.

2. INTRODUCING COMPETITION

The introduction of competition into the operation of the DNS has been one of the most important goals of the Clinton administration's "privatization" campaign. Competition was one of the four basic principles set out in the U.S. Green Paper, along with stability, private bottom-up coordination and representation — and it remains so in the U.S. White Paper. While there is widespread support for competition in principle, disagreement exists over how best to introduce competition in practice. Moreover, concerns have been expressed about whether it will be sustainable if certain conditions come into play under current American proposals. For its part, the Government of Canada supports the principle of competition in the DNS, though not in any form or at any price.

Where Competition Fits

To understand how competition fits into the picture, it may be helpful to consider three contrasting levels of activity: the Internet vs telecommunications in general, the DNS vs other Internet-related functions, and the naming vs addressing functions of the DNS.

By contrast with other areas of telecommunications like cellular and long-distance telephony, the calls for promoting competition in the DNS have not come about because of concerns over making services affordable to consumers, nor because of the desire to promote technical innovation and growth in new markets. The Internet has not reached a watershed divide because of undisciplined pricing in the DNS arena — though criticisms have certainly been voiced over the pricing of other elements of Internet operations, like backbone facilities and end-user connectivity. Still less have Internet users and governments worried about a lack of technical innovation or low consumer demand — though continuing technical innovation is of course an important policy goal of both the Canadian and American governments. On the contrary, the problems prompting calls for reform, as noted above, have almost entirely to do with dramatic growth and a changing user population, including an increasing number of both mainstream business users and international (i.e. non-American) users.

As far as competition is concerned, moreover, an important distinction has to be maintained between the DNS and other Internet-related functions.

In two major Internet areas, namely content and connectivity, there is meaningful competition. Low entry barriers, increasingly sophisticated browsers and other software, access to a global user population and the ease with which content on the Internet can be transmitted, have all conspired to make Web publishing feasible to huge numbers of businesses and individuals — as witness the current total count of pages on the Web, some 300 million, along with a staggering variety of commercial and non-commercial content. In the course of 1998, competition has become particularly fierce among the large, heavily trafficked sites known as portals, which are battling to win visitors and the advertising revenues that go with them. Similarly, the markets for both commercial and residential connectivity are thriving in Canada and elsewhere, while interest in providing connectivity has extended from specialized computer firms to the major providers of telephone and cable service. These attributes of the Web, and the growing volume of activity, are important factors in the long-term development of e-commerce.

Although the naming and addressing functions of the DNS are intimately connected, the proposed introduction of competition is essentially confined to the naming functions of the DNS. Competition would be introduced to the DNS name space, i.e. to the management of TLDs and the issuance and maintenance of SLDs by a number of for-profit firms. Little or no support exists for the idea that the issuance of IP address blocks should be handled on a commercial, competitive basis. Nevertheless, certain changes are being discussed in the way ARIN and its sister agencies carry out the tasks associated with the assignment of IP address blocks, such as the size of blocks that can be allocated and therefore the size and importance of the organizations they have direct dealings with (currently large number blocks are allocated to large institutions within each region, then progressively reallocated among smaller groups). Concerns have been expressed that while the current handling of IP address blocks is satisfactory, the potential exists for anti-competitive behaviour in this area, especially given the uncertainties about future changes to the system.

Current discussions of competition have highlighted the distinctions between the DNS functions carried out by registries on the one hand and registrars on the other. The role of a registry is to act as the technical, legal and commercial home of one or more top level domains. The role of a registrar, on the other hand, is to issue SLDs to applicants on behalf of a registry. Since it took over aspects of DNS management in 1992 on a monopoly basis, NSI has acted as the sole registry of the most popular and important TLDs, namely .com, .net and .org. NSI has also acted as its own registrar, dealing with applicants and registrants either directly or through intermediaries like Internet service providers (ISPs). In Canada, many ISPs handle domain name registration on behalf of their subscribers for a fee typically of between $50 and $75 (over and above the fee charged by NSI).

Over the last couple of years, a handful of organizations have tried, with varying degrees of success, to introduce their own TLDs, operated through proprietary registries — e.g. the high-profile name.space, AlterNIC and eDNS mentioned in the White Paper, as well as a number of others that have had varying degrees of success in establishing themselves: .agn, .earth (American GlobalNetwork); .idg (International Data Group); .auto, .web (Image Online Design); .biz, .corp, .usa (MCS Net); .alt, .post, .live (Memra Software); .eur (NetNames); .art, .ent, .sex, .sky (Skyscape Communications); .fcn (Free Community Network). Not all these would-be registries are entering the DNS market because they see an opportunity to make money. The last in the list (Toronto-based .fcn) is in fact a not-for-profit that has tried to provide free connectivity to other civic-minded organizations.

Registrars & Competition

In the course of the Canadian and American consultations on the DNS, few objections have been raised to the idea of allowing competition among registrars. The consensus view is that registrars should be free to operate, on a commercial basis or otherwise, as agents for any or all of the available TLDs. But several questions can be raised in conjunction with such a scenario. It should be emphasized that these and many other questions raised in this paper are to be examined and eventually answered by the new corporation — and, as noted below, this raises further questions for the Canadian

government as to how the new corporation will be held accountable for the solutions it proposes.

What minimum requirements should potential registrars have to fulfil?

The appropriate policy goal would appear to be to strike a balance between the need for a technically sound, efficient and secure operation, and the desirability of opening the market to a broad range of potential supplier firms. In other words, the formal entry criteria shouldn't be either too rigorous or too lax.

How should registrars be chosen?

Apart from formal criteria, there is some difference of opinion as to whether registrars should be allowed to enter and leave the market freely, or whether further constraints should be placed on entry through a selection process. In policy terms, the goal of full and effective competition suggests that the door should be left as open as possible. This issue is closely connected with the next question concerning operating rules imposed on registrars.

What formal restrictions should be placed on the activities of registrars?

If registrars were allowed to operate without a generally accepted set of rules, consumers might be exploited and the stability of the Internet might be placed in jeopardy. Certainly, given the pro-competitive goals underlying this whole exercise, the first policy concern should be rules to prevent *anti*-competitive behaviour by registrars — for example, any actions designed to hold customers captive by making it difficult or expensive to move their business to another registrar. The Canadian Domain Name Consultative Committee (CDNCC), which is currently responsible for an overhaul of the .ca domain, has addressed this and other questions in its rules about agents. While the CDNCC proposes to open the registrar market up for competition, it is nevertheless stipulating minimum technical, operational and financial requirements for registrars, in order to maintain the integrity of the .ca domain. Once again, a balanced policy is needed, one that stimulates

growth at the registrar level and yet provides adequate protection for businesses and consumers that use the services of registrars.

Registries & Competition

The competition scenario is quite different as it relates to registries. As the home of a root server that handles one or more TLDs, a registry performs critical technical functions and holds vital information about routing, addressing, customers and updating, among other things. The stability of the Internet and the welfare of many of its users depend on the secure, reliable and responsible execution of a host of registry functions.

What are the arguments against competition at the registry level?

The consultative process has not produced the consensus on registry competition that has been achieved on registrar competition. Despite the benefits anticipated from competition, the operation of competitive registries is likely to increase, not reduce, the technical challenges associated with interoperability, security and reliability. Moreover, some stakeholders see a competitive and for-profit registry system as anomalous, arguing that registries should be operated as a public trust, not as for-profit commercial concerns. According to the public trust argument, the overall goal of governance should be to enhance the welfare of all those who operate and use the Internet, and to ensure the best possible technical development of the Internet, not to create money-making opportunities for some individuals at the expense of others. Some commenters have taken this view one step further, arguing that as a public trust, Internet governance should remain in the hands of government and officials who are at least indirectly accountable to elected lawmakers.

One other leading argument has been made against the idea of competition at the registry level and that concerns domain name portability. This issue is analogous to one of the problems raised by competition in local telephony: even with the prospect of lower prices and better service, many customers, especially business customers, are reluctant to give up a telephone number they have been associated with for an extended period of time. Like number portability, domain name portability would allow a user to switch from one provider, or registry, to another, without giving up a particular name or suffering any

penalty or undue switching cost. However, such a system requires not only that the technology be in place to handle switching, but also that registries be compelled to refrain from "locking in" or penalizing customers that do elect to change providers or registries.

The Canadian government is generally supportive of any mechanism or technology, such as domain name portability, that will allow competition to operate in a way that enhances business opportunities while also protecting customers.

What are the factors pushing towards competition at the registry level?

First, the U.S. government is strongly in favour of registry competition, despite the various drawbacks. It has not only made competition the overall goal of reform, but has explicitly suggested that the new corporation should organize a new system of registries along competitive lines. Thus, while deferring to the new corporation on this and many other issues, the White Paper states (section 6) in connection with registries that "competitive systems generally result in greater innovation, consumer choice, and satisfaction in the long run. Moreover, the pressure of competition is likely to be the most effective means of discouraging registries from acting monopolistically."

Moreover, pressure for the creation of new registries has come from several other quarters, including those who have already launched independent efforts as registries; those who have expressed dissatisfaction with the NSI monopoly; and those who see new TLDs as an important way to stimulate the overall growth of the Internet and of e-commerce in particular.

Finally, pressure has come from outside the United States, especially international stakeholders and other countries, including Canada, which see competitive registries and especially the creation of new TLDs as a way of making the American-led reform and American-based corporation more accountable to and representative of the international community.

Are there benefits to be gained from a DNS that is competitive but not necessarily or entirely for-profit?

Even if the new system is likely to be competitive, and competition is introduced through the creation of new registries and new TLDs, not all operators would necessarily want to offer service on a for-profit basis. There may, for example, be charitable, artistic or religious groups that are prepared to manage a new domain for reasons other than commercial gain. While such groups must be prepared to show they have the financial and technical support necessary to offer dependable service, the Canadian government believes the new system should be flexible enough to allow for this kind of diversity.

3. THE ROLE OF THE NEW CORPORATION

Overhauling DNS management raises difficult questions about balancing the need to coordinate complex DNS functions across the Internet in a way that maintains stability, with the need for governance that is accountable in some fashion to the many user communities. As noted above, a number of stakeholders have criticized the DNS governance model being advanced by Washington — i.e. a private, not-for-profit corporation not controlled by government, yet charged with a broad mission of public trust based on democratic principles.

In opposition to the "public trust" view, that the management of the DNS should continue to be entrusted to an agency of government, it can be argued that the process set in motion by the White Paper requires fresh thinking about private- and public-sector responsibilities. It may be that some hybrid model akin to a "private trust" will emerge from the current discussions, one that manages to capture the rather unusual ability of Internet coordinating bodies to work in a way that ultimately serves the public interest, yet has no built-in democratic procedures, at least not of any traditional kind.

Even under an optimistic view of prospects for the new corporation, the White Paper model does raise an issue for some stakeholders about the creation of a competitive DNS marketplace through the agency of a central body that has monopolistic decision-making powers. These concerns have been compounded by two factors. First, the U.S. government wants to remove any government-imposed public oversight such as that typically provided by tribunals or agencies that are ultimately accountable to elected lawmakers. This is of course the heart of Washington's whole rationale for "privatization" or devolution to the private sector. And second, despite providing some details about the makeup of the new corporation, the White Paper has deferred many questions to that body and created uncertainties about how it will behave in the marketplace, without reference to explicit safeguards on the exercise of what may be extensive, monopoly-like powers.

Whether or not the new corporation behaves in a truly pro-competitive and democratic spirit is likely to depend on two quite different kinds of safeguards, one narrowly legal,

the other going to more fundamental aspects of governance. The first of these is antitrust law; the second involves how to make the new corporation accountable — and to whom. On the basis of the vague proposals put forward in the White Paper, the Government of Canada has concerns about the accountability of the new corporation, as well as about whether and how it will be representative of international interests, including mainstream, non-American business groups.

Antitrust Issues

A number of stakeholders have raised concerns about the extent to which U.S. antitrust law will or will not apply to the new régime. The White Paper policy response is to reject the idea of indemnifying the new corporation against antitrust challenges and to provide assurances that applicable antitrust law — and the threat of lawsuits — will prevent abuses of power. Once again, it is difficult to assess the principle behind this statement before knowing exactly how either the interim or permanent board of directors will structure its affairs.

The White Paper envisages that by behaving along the lines of a standards-setting body, the new corporation is likely to be less vulnerable to antitrust challenges. The model is described as follows (section 9):

> Under this model, due process requirements and other appropriate processes that ensure transparency, equity and fair play in the development of policies or practices would need to be included in the new corporation's originating documents. For example, the new corporation's activities would need to be open to all persons who are directly affected by the entity, with no undue financial barriers to participation or unreasonable restrictions on participation based on technical or other such requirements. Entities and individuals would need to be able to participate by expressing a position and its basis, having that position considered, and appealing if adversely affected. Further, the decision making process would need to reflect a balance of interests and should not be dominated by any single interest category.

While the Canadian government finds merit in this model, it notes there are no explicit provisions in the White Paper to oblige the interim board to implement such a model, apart from the negotiating process that is expected to take place as part of the handover.

To what extent will Canadian interests be protected by American antitrust sanctions?

Canadian competition law operates under a different set of assumptions from American antitrust law. Canada's *Competition Act* does contain some provisions which may apply to the conduct of foreign corporations in Canada, but application of these provisions requires a clear nexus with Canada. Whether or not any of these provisions would come into play in the event of a claim or suit against the new corporation will depend on the particulars of its articles of incorporation and its future role in Canada, among other things. While Canadian interests may be represented in antitrust lawsuits launched in the United States, it is clearly in Canada's best interest to see that Canadian nationals and their businesses are protected from untoward exercises of power, just like American nationals.

Is the threat of civil litigation an appropriate safeguard against potentially anti-competitive behaviour?

In the absence of other safeguards, the threat of legal challenges in the United States alluded to in the White Paper is a useful condition for disciplining the behaviour of the new corporation. But it doesn't go far enough — and it has a serious drawback for Canadians. The drawback is that Canada's *Competition Act* may facilitate some civil actions, but such litigation in the courts is expensive and burdensome. Civil antitrust lawsuits are simply more developed in the United States than in Canada. For Canadian and other internationally based organizations, litigation may prove to be a necessary last resort, but finding ways to prevent anti-competitive behaviour in the first place is clearly superior. That involves careful attention to the issues of accountability and representation.

Accountability & Representation

The reform of the DNS is taking place at the juncture of what might be described as top-down policy-making and bottom-up coordination. Government officials are preparing to hand off responsibilities to the private sector through a transition process that as yet has no clear outcome, a process that is being led but not entirely directed by government. The "private sector" is in fact a heterogeneous collection of Internet coordinating bodies, user groups and other special interests who not only do not speak with one voice, but who in many cases are used to working in small committees operating by the credo "rough consensus and running code." This combination of factors has created considerable uncertainty, and the criticism from some that the Internet "community" — already known for its factiousness — is being asked to agree on a proposal for reform that raises far more questions than it answers.

The Government of Canada shares these concerns, especially on the subject of the structure and role of the new corporation. At the level of general principles, the White Paper is reasonably clear on the kind of corporation it intends to see established. In addition to the Green Paper principles of stability, competition and private bottom-up coordination, the White Paper highlights representation as a key principle going forward. That is, the U.S. government has quite rightly recognized that it is in the best interests of all concerned, as well as best for the stable functioning of the Internet, if the new corporation is constituted in a way that ensures broad representation — including representation of non-American interests. The White Paper underscores this point (section 11):

> The U.S. Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management.

The new corporation is to be run by a 15-member board that will make many important policy decisions deferred by the U.S. government. It is to be comprised of three representatives of regional number registries, two members designated by the Internet Architecture Board (IAB), two members representing domain name registries and domain name registrars, seven members representing Internet users, and the Chief Executive Officer.

The seven "user" representatives will clearly play a crucial role in achieving the goals established for the new corporation — including whether or not the corporation is likely to act in a way seen as accountable to those whose livelihoods are coming increasingly to depend on stable growth of the Internet. Another crucial aspect of the new corporation's governance structure, as outlined in the White Paper, is the proposed use of advisory councils:

> The new corporation could rely on separate, diverse, and robust name and number councils responsible for developing, reviewing, and recommending for the board's approval policy related to matters within each council's competence. Such councils, if developed, should also abide by rules and decision-making processes that are sound, transparent, protect against capture by a self-interested party and provide an open process for the presentation of petitions for consideration. The elected Board of Directors, however, should have final authority to approve or reject policies recommended by the councils.

The Canadian government believes such a system of councils could provide an excellent forum for the airing of minority views, resolving disputes and preparing advice to the board on complex technical matters.

On this matter of the councils and many other governance issues, however, the White Paper has left far too many questions in limbo. There is no description of how the new corporation will be selected, a process that so far is being left entirely to bottom-up initiative. Similarly, there is no provision made on several other crucial issues: how board members will be selected, i.e.whether they will be elected and if so, by whom; to whom the board will be accountable, and particularly the nature of the ongoing relationship between the board and the U.S. government; whether and in what manner the board will

be legally responsible to a membership; and whether the proposed board membership structure is appropriate, given the suggested balance between technical and non-technical members.

Are the proposed arrangements for structuring the new corporation likely to strengthen or weaken Canada's voice in DNS management?

If the White Paper proposals are carried through, there will be no representation of governments, except in a non-voting advisory capacity, on the board of directors. In other words, neither Canada nor other "sovereigns" will have a direct voice in DNS governance at an official level. This minimal role for government is in keeping with the overall rationale for reform, which is to turn management over to the private sector.

On the other hand, this principle of representation may make it more difficult for international, i.e. non-American, interests to assert their rights and exert influence over the decision-making process. The Canadian government wishes to ensure that Canadian organizations with an interest in DNS governance will find a way to make their voices heard at the corporation. The government intends to lend support to these interests throughout the discussion process not only by participation in international forums on DNS-related issues, but also by releasing information bulletins to keep concerned members of the public abreast of new developments.

Since the release of the White Paper, a number of international consultations have been held or are being planned, with a view to gaining some consensus on how to proceed.

The International Forum on the White Paper (IFWP) played a role in organizing the first of a proposed series of workshops, this one having taken place in Reston, Virginia on July 1 and 2, 1998. Most of the key stakeholder groups were represented in some fashion, including ARIN, CAIP (Canadian Association of Internet Providers), CIX (Commercial Internet Exchange Association), IANA, CORE (Council of Registrars), ISOC (Internet Society) and NSI, in addition to presidential Internet advisor Ira Magaziner. This is how the Forum Web site <www.giaw.org/> describes the mission:

> The workshop is intended — in spirit and letter — to fully meet the requirements specified in the Dept. of Commerce, NTIA Proceeding Policy Statement on this subject. However, it is not the purpose of the workshop to actually create The Entity, but only to bring all the stakeholders and experts in corporate law and organization together to provide the basis for subsequent creation. This is believed to provide as neutral and inclusive a setting as possible for stakeholders of disparate views.

It is not clear, despite the good attendance at the Reston meeting, that any real progress was made even on the modest goals noted in the mission statement. As this paper is being written, further international workshops are being planned.

4. TOP LEVEL DOMAINS

Earlier, some discussion was devoted to the prospect of new TLDs competing with the "generics" managed over the last five years by NSI. This section looks a little more carefully at some of the details — including some differences between the status of gTLDs like .com and ccTLDs (nTLDs), comprising over 200 country codes or national top level domains, like .ca.

Generic Top Level Domains (gTLDs)

A number of earlier reform proposals, including those issued by Jon Postel and IAHC (International Ad Hoc Committee), as well as those contained in the Green Paper, argued in favour of adding new TLDs to those already in use. And several experimental and largely unsanctioned TLDs have been in use for some time, though with only limited reach among Internet users, as noted earlier. But there was, and still is, sharp disagreement over whether adding new TLDs to the system would bring benefits or harm. In contrast to the position taken by the Green Paper, the White Paper has left the question of whether new TLDs should be created entirely to the new corporation.

Like other members of the international community, Canada has an interest in seeing that any new DNS system be set up in a way that delivers benefits across the widest possible range of users, especially outside the United States. Thus, the Canadian government supports the basic principles of introducing competition and minimizing government involvement in the actual running of the DNS. The reform process should be used to help stimulate business development in Canada — in the short term through DNS-related opportunities and in the longer term through removal of barriers to the growth of e-commerce.

In practice, this means that Canadian groups, both commercial and non-commercial, should have some opportunity to come forward with entrepreneurial proposals for the operation of both registrar services and registries. Some will wish to do so through the introduction of new gTLDs. According to this view, Canada may have some interest in at least a modest experiment with a competitive registry system incorporating new TLDs.

This would in principle allow Canadians to control the policy and technical aspects of a fundamental part of the DNS, thereby giving those involved a voice in the wider deliberations of the new corporation.

Others disagree with this view, questioning just how far the assumed benefits of creating new TLDs would extend, apart from creating business opportunities for new registries and suppliers of names. One of the reasons most often cited for creating new domains is, of course, opening up competition. But according to those who oppose new TLDs, the addition of new domains will be self-defeating, because many businesses will simply register their trade-marks across as many domains as they feel is necessary to protect their interests. The more domains to be registered, the more business for registries (and registrars) — but the greater the expense for those wishing to do business online.

Where do Canada's interests lie in this area?

While uncertainty continues to hang over the issue of new registries and new TLDs, many parties seem to be in agreement with the need for careful, well calculated expansion of the name space — and the need to keep a watchful eye on possible technical problems, since even short-term problems like name lookup failures or name collisions can have a highly detrimental effect on the welfare of users. As the White Paper notes (section 7), "a prudent concern for the stability of the system suggests that expansion of TLDs proceed at a deliberate and controlled pace to allow for evaluation of the impact of the new TLDs and well-reasoned evolution of the domain space."

While not necessarily subscribing to all the arguments for new TLDs, the Government of Canada believes that the pressure for adding domains is likely to win out and that Canadians with a stake in this issue should be prepared for this eventuality. The government further believes that if new domains are added under the emerging régime, then one or more new registries should be based in Canada, with some measure of control and the accompanying benefits being extended to Canadians.

Country Codes (ccTLDs)

An important factor in assessing the wisdom of increasing the number of gTLDs is the widespread use — outside the United States — of national level TLDs or country codes (ccTLDs). The more than 200 such TLDs are mostly based on the two-letter codes established by the International Standards Organization (ISO) as an international standard for other naming purposes.

One of the general difficulties for the White Paper implementation process lies in the contrasts between Internet practices and expectations in the United States, and those in other countries. Apart from the much higher presence of hosts and users in the United States, and the fact that the coordinating bodies have been funded by U.S. agencies, another discrepancy exists in the use of TLDs: users in the United States have almost entirely avoided the American country code .us in favour of the gTLDs, whereas the ccTLDs are an important part of the Internet addressing structure in many other countries.

Lack of use of .us may help to explain why the White Paper is almost silent on the subject of country codes. It does state (section 4) that "national governments now have, and will continue to have, authority to manage or establish policy for their own ccTLDs." As noted earlier, however, it also states that "the U.S. continues to believe, as do most commenters, that neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses." Later in the document, the proposal is made to seek comment on extending the commercial use of the .us domain. Although the issue of the .us space has a high domestic priority for the U.S. government, it is regarded as much less important in the context of international consultations.

Is there a rationale for independent policies on country codes?

There are several reasons why the American approach to use of the .us domain, and to the country code space in general, should not be taken as a model for other countries, including Canada. First, the actions of the new corporation may have a bearing on how ccTLDs are integrated into the DNS overall. The development of these policies and

procedures must be watched closely, with international interests in mind. Second, a number of ccTLDs — such as .tm (Turkmenistan) and .nu (Niue) — are being marketed and used very much like de facto gTLDs, a trend that is eroding some of the differences between the two TLD types. This too is a trend that bears careful monitoring.

A third and crucial reason for an independent ccTLD policy involves the work under way in Canada on the .ca domain and its potential importance for Canadian Internet users. Canadians have an interest in preserving a .ca domain space that will function well into the future, and its viability may depend on a technical and administrative structure that departs from general principles laid down for the DNS by the new corporation (within allowing for full interoperability across the Internet as a whole).

Over the course of 1997-1998, the Canadian Domain Name Consultative Committee (CDNCC), undertook responsibility for a proposed overhaul of the .ca domain. The committee, which operates with the participation of the Government of Canada (represented by Industry Canada), has developed new rules for registration in and administration of the .ca name space, in part because of pressure from new users for a more streamlined and liberal system — one closer to the principles established by NSI for .com, including rapid registration on a first come, first served basis. It is proposed that implementation of the new .ca system be handled by the Canadian Internet Registration Authority (CIRA), which will operate on a not-for-profit basis.

The CDNCC's initial public consultation on the .ca name space seems to have been successful, in terms of both comments received and the solutions developed for responding to concerns. Some of the new procedures established in the Canadian reform process may now provide useful guidance in the international deliberations on the White Paper — such as a role for government oversight within a domain name structure shaped by the private sector (the proposal stipulates a permanent, non-voting, ex-officio seat on the new registry); efforts to ensure that key stakeholders are represented; and reliance on an open, consultative process in decision-making.

The CDNCC is proposing fairly rigorous Canadian requirements for registrants, registrars and registry board members. Significant effort is being put towards balancing the need for

a system compatible with the open, international nature of the Internet, with the objective of keeping the .ca domain a resource owned and controlled by Canadians for Canadians — clearly a policy approach of fundamental importance to the government.

See <www.canarie.ca/cdncc/> for further details on the CDNCC process.

5. ADDRESSING & RELATED TECHNICAL ISSUES

As suggested earlier, the greatest pressures for change in the DNS have come about as a result of the commercialization of the Internet, along with the influx of new users around the globe over the last couple of years. In contrast to the specialist technical community that helped to create ARPANET and then the Internet itself, most of these new users have little if any interest in the technical underpinnings of the Internet. Their primary interest, whether as casual users, registrants or organizations caught in disputes, is the names they see and use everyday in Web and email addresses.

For the most part, therefore, public attention has been more focussed on the name space than on the address space and the status of the IP numbering system. Nevertheless, the White Paper makes it clear that part of the new corporation's central mandate is to "set policy for and direct allocation of IP number blocks to regional Internet number registries" (Principles for a New System). Among those concerned over the future of the address space, a caution has been raised over the relative weight being given to the two sides of the DNS debate.

Relative Importance of the Name & Address Spaces

As this argument goes, domain names are actually less of a real-world issue for everyday users than the current debate would suggest. Trade-mark disputes and other conflicts aside, anecdotal evidence suggests that ordinary users rarely access Web sites, for example, by typing in the full URL (uniform resource locator), the Web address based on the domain name of the individual or organization that operates the site in question. It has became much more common for access to take place in an automated or semi-automated way — through bookmarks, hot links from email or other Web sites, and pointers provided by search engines, which are now among the most popular destinations on the Web.

To many end-users, the domain name appearing in Web addresses may be unknown and of little interest to them, aside from a certain number of highly popular Web sites. Yet they can still avail themselves of other methods for getting to their desired destinations.

Furthermore, although concerns have been expressed that the .com domain in particular is rapidly being exhausted, many other creative avenues are open for expanding the potential pool of names. Some proposals are being discussed for making domain names even less critical for Internet traffic by providing comprehensive directory resources.

The same cannot be said for the address space, which is a highly structured software resource to which domain names must be mapped in a precise, consistent and non-ambiguous way. The interoperability and robustness of the Internet are heavily dependent on the numbering scheme that is used for addressing and any changes to it must be implemented under the guidance of the coordinating bodies involved, particularly IANA, the IETF and IAB, as well as the regional IP registries. The nature of the IP numbering scheme, combined with the exponential growth of Internet use, have caused some stakeholders to declare the address space a scarce resource and to warn that plans must be put in place quickly before it is exhausted.

There is certainly nothing like general agreement over the scarce resource theory. More powerful computers and networking equipment have reduced much of the technical strain on the DNS, such as the speed with which mail servers can check lookup tables to route ever-growing volumes of email. Moreover, some implementation has already begun of the next version of the Internet protocol, known as IPv6, which is intended to replace the current version, IPv4.

IPv6 would create a vastly greater IP numbering resource, because it has been designed on the basis of 128-bit addressing technology, as opposed to the 32-bit technology utilized by IPv4. But a good deal of uncertainty has developed around its implementation and IPv6 may not be in general use for many years. Just how the scarcity argument plays out is also fraught with uncertainty. On one hand, the address space is now used much more efficiently than in the past, while on the other hand, the near future may see a huge surge in the demand for IP numbers, as not just computers but game consoles, TV sets, even household appliances become addressable.

How does the current addressing system affect Canada and what is the Canadian position on proposed changes?

Whether the IP address space is regarded as a scarce or only "limited" resource, the fact is that Canada does not directly control the assignment of IP number blocks, as it once did. Control of assignment was given up in April 1996 by the University of Toronto largely because upgrading the technical infrastructure to then current standards would have been prohibitively expensive. Control was ceded first to InterNIC and subsequently to ARIN, which now controls the assignment of number blocks for North and South America.

Although the system as operated by ARIN has performed satisfactorily up until now, the system will undergo changes as the new corporation gradually takes over the DNS management functions associated with addressing. In order to ensure that Canadian interests are protected, it has been suggested by some that the assignment of large blocks to Canadian institutions should be repatriated and once again brought under the control of a Canadian body. This body would help ensure, for example, that Canadian users, including .ca registrants, would benefit from IP assignments based on blocks of sufficient size, contiguity to other specified blocks and so on. This idea stems in part from concerns that the new corporation may not be sufficiently sensitive to the needs of non-American institutions as it introduces changes into the addressing system.

Several factors make it difficult to determine Canada's best position on this issue. First, while repatriation of number block assignments may have benefits to Canadians, the functions involved require a high level of technical infrastructure and expertise, including fully secure and redundant computer systems, with high bandwidth requirements. It is not clear how the associated costs would be supported in Canada, given that neither public- nor private-sector funds have been identified for this purpose.

Moreover, there is considerable confusion over the issue of ownership of the address space, i.e. ownership of the number blocks assigned to large corporations and other institutions like universities. The argument has been made that after years of use of large number blocks, the incumbents have ownership claims over the numbers — claims that

may conflict with the rights and operations of the regional registries, as well as those of other Internet users.

In view of these and other uncertainties, any changes to the addressing system deserve careful study by a broad cross-section of international interests, not just the bodies which have special jurisdiction in this area, like IANA and ARIN. That would include experts who have a more general role to play in looking after the health of the Internet. These issues would be well suited to discussion within the proposed advisory council structure.

6. TRADE-MARKS & DISPUTE RESOLUTION

One of the most contentious areas of disagreement in the DNS debate has divided domain name registrants and owners of trade-marks, trade and corporate names, and other intellectual property. Trade-mark conflicts raise particularly acute jurisdictional issues and have divided American and non-American interests. Here again, a nascent conflict has come to the surface because the commercialization of the Internet has brought millions of new users into the picture who have widely divergent interests when it comes to name registration and the use of names and addresses online.

One of the chief sources of conflict has been the long-established practice of NSI whereby users could be assured of fast, relatively inexpensive registrations of SLDs on a first come, first served basis — with no requirement that the registrant justify use of a particular name (such as demonstrating a legal right to its use); no provision for the settling of disputes when they arose; and no requirement that any payment be tendered to NSI before the registrant began use of the name. These practices led to instances of name hoarding, frivolous registrations and "cybersquatting" — holding on to SLDs to deprive other, legitimate parties of their use, often with a view to profiteering by selling the names back to these parties for an inflated fee.

Despite such anti-competitive practices, the NSI framework can be credited with serving the public interest in certain significant respects — encouraging the rapid growth of the Web, innovative uses of Web sites, and the acceptance by business and consumers of the Internet as a fundamental part of the North American economy. There is, therefore, a policy trade-off between low entry barriers, such as making registration fast and easy, and the protection of legitimate business interests, in this case the right to use certain trade-marks and to contain and punish infringement. Like many other parties, the Canadian government wants to see a balance struck between these competing goods, so that growth can be sustained and conflicts kept to a minimum.

Adding to this policy dilemma is a fundamental discrepancy between the application of trade-mark law in Canada (and other jurisdictions) and the scope of SLDs. In trade-mark law, a name or mark is usually associated with specific wares or services. It is possible

for a trade-mark such as "ACME" to be used legitimately by one company in association with a dry cleaning firm performing dry cleaning services and by another company in association with the resale of computers. In long-standing DNS practice, however, names like "acme.com" can be registered and used without any restrictions being placed, implicitly or explicitly, on the scope of their application. And to compound the problem, trade-marks are validated and regulated nationally, whereas domain names are international in their scope.

Until the Internet was well into its commercial phase and graphical Web browsers came into widespread use, trade-mark infringements were not regarded as a particularly serious issue. As long as the Web continued to be a marginal communications vehicle incorporating little or no business activity, any potential harm flowing from trade-mark infringements was mitigated by their near invisibility — at least compared to infringements in mainstream media like the daily press and television. All this changed, however, as business investments grew in Web sites, Web advertising, and technologies and content associated with electronic commerce. And the stakes went up even further as companies trading under famous brands, like a Disney or a McDonalds, began to see the implications of allowing a Web site to operate using their name without permission. Conflicts grew more numerous, while mechanisms for settlement, outside of expensive litigation, remained remote.

What are the current proposals for dealing with disputes and related intellectual property issues?

Both the Green and White Papers set forth proposals for dealing with disputes and balancing the interests of domain name and trade-mark holders. Commenters on the Green Paper found fault with a number of its proposals, some of which have been modified accordingly in the White Paper.

The most important of the White Paper proposals is the call for an international process to be convened by the World Intellectual Property Organization (WIPO), based in Geneva, whose purpose would be to solicit recommendations on the trade-mark and other intellectual property issues associated with the DNS. WIPO responded with alacrity,

issuing an initial Request for Comments (RFC-1) on July 8 intended to gather comments from interested parties on the proposed terms of reference of the process (details available at <http://wipo2.wipo.int/process/eng/processhome.html>).

These terms of reference follow the general outline provided in the White Paper, both emphasizing the importance of finding widespread agreement on a uniform alternative dispute resolution mechanism, in order to reduce reliance on court litigation. But the WIPO RFC departs from the White Paper in two respects, one a matter of structure, the other a matter of scope.

First, the RFC, like the White Paper, lists three main areas of inquiry: dispute resolution, the protection of famous marks and the potential impact of adding new TLDs. But the RFC makes a clear distinction between the *resolution* of actual disputes involving the DNS (through alternative procedures to be discussed) and the *prevention* of such disputes. Both documents refer to the use of readably searchable online database information about registrants to avoid conflicts and expedite settlements without resort to the courts. Most registries and registrars, including NSI and the membership of CAIP, do not wish to be involved in third-party disputes. The Canadian government believes, however, that as a reasonable compromise, registries and registrars should provide database information as a service to registrants and trade-mark holders. As the White Paper puts it (in Revised Policy Statement):

> Trademark holders and domain name registrants and others should have access to searchable databases of registered domain names that provide information necessary to contact a domain name registrant when a conflict arises between a trademark holder and a domain name holder.

The White Paper goes on to explain (in the accompanying footnote) that "these databases would also benefit domain name holders by making it less expensive for new registrars and registries to identify potential customers, enhancing competition and lowering prices." The RFC mentions the additional possibility of creating directory and listing services that may allow identical names to co-exist on the Internet. The Canadian government generally endorses any such mechanism that is likely to contribute to the

prevention of disputes, while not creating hardship, financial or otherwise, for any of the parties involved.

But the more significant departure of the RFC lies in the proposed scope of the inquiry, which is to be considerably broader than that suggested in the White Paper. For example, the White Paper states unequivocally (section 8) that:

> ... whatever dispute resolution mechanism is put in place by the new corporation, that mechanism should be directed toward disputes about cybersquatting and cyberpiracy and not to settling the disputes between two parties with legitimate competing interests in a particular mark. Where legitimate competing rights are concerned, disputes are rightly settled in an appropriate court.

The Government of Canada believes that this proposal places an inappropriate and unworkable restriction on the models that may be considered for alternative dispute resolution mechanisms. Consequently it supports the suggestion made in the RFC that the inquiry explore "[w]hether some or all of the above dispute resolution approaches should be restricted to cases involving cyberpiracy or be available also for conflicts between trademark holders with legitimate competing rights." The government generally wishes the WIPO inquiry to be made as broad and representative as possible.

The White Paper mentions one additional principle that deserves endorsement: namely that registrars should be required to collect payment from registrants before they are allowed to use any domain name. As noted earlier, the delayed payment system established by NSI has led to abuses and concrete benefits are likely to flow from an upfront payment system, with little risk of hardship or unfairness to any registrant.

7. ROLE OF GOVERNMENT & THE PRIVATE SECTOR

As stated in the White Paper, the U.S. government's goal is complete withdrawal from any direct role in DNS management once the transition period is completed. Its policy is also to prevent representatives of other sovereign nations from playing any direct role in governance. These policy goals raise questions about the appropriate role of government in general and the Government of Canada in particular.

It should be noted, first of all, that the handoff of DNS management functions to the new corporation will not happen all at once. The White Paper calls for a transition process to begin this October, with the appointment of an interim board of directors to set up the new corporation. The entire transition is expected to last about two years. "To the extent that the new corporation is established and operationally stable," states the White Paper, "September 30, 2000 is intended to be, and remains, an "outside" date." The White Paper outlines five major tasks for the transition: the ramp-down of NSI's role as the monopoly provider of DNS service; conclusion of an agreement between the government and the new corporation; launch of the WIPO dispute resolution process; consultation with the international community; and review of the root server system.

During this period, it is clear that the U.S. Government will have a major role to play in shaping the transition, defining the makeup of the new corporation and making representations to international forums like WIPO and the OECD (Organization for Economic Cooperation and Development). What is not as clear is how the interests of countries other than the United States will be protected and what residual role government should have after the transition period is complete.

Part of the answer lies in the role being assumed by the "private sector." In Canada and elsewhere, the private sector side of discussions is being led not just by the established Internet coordinating bodies, but by a number of commercial stakeholders as well, some quite new to Internet-related issues. This broadening of the scope of stakeholder interests is entirely appropriate and should continue. Indeed, one of the Canadian government's primary goals in this whole process is to make Canadians aware that as business people, consumers and citizens they have much to gain from understanding how the evolution of

the Internet will affect their lives in the coming years. And while it has its arcane technical side, the proposed changes to management of the DNS have social implications that are quite properly being debated on a wider public stage.

Although the DNS reform is being led by Washington and national governments will not have direct representation on the board of the new corporation, the Canadian government has been taking an active role both domestically and internationally as the process unfolds. This role has taken several different forms: expert analysis of the emerging technical, legal and policy issues; representation at American and international forums; a watching brief in areas like standards development that have traditionally seen government involvement in technical administration; and a public education and industry support role at home.

This monitoring and support role being played by the Government of Canada is in no way intended to substitute for the increasingly active contribution of the private sector. DNS and Internet related issues are quite clearly to be handled by the private sector, except where there is agreement among the stakeholders that the public interest will be better served by limited government involvement. The key is to find a balanced and flexible approach that will allow the government to promote the healthy growth of the Internet and electronic commerce without actually directing or regulating the activities of Canadians in their online endeavours. Two illustrations might help suggest an overall direction.

First, the government wishes to ensure that the framework developed for management of the DNS and Internet governance in general is consistent with applicable Canadian law, such as provisions of the *Competition Act*. This principle means that Canadians should be confident that in their day-to-day activities as online consumers and business people, they are protected by a consistent and stable set of rules that creates no unexpected gaps or conflicts. And this principle means that government has an obligation to keep a watchful eye on the constant ebb and flow of changes in online technology, commerce and the law — and to take actions domestically and internationally that will continue to ensure that Canadians benefit from a stable framework for management of the DNS and Internet governance.

A second and related reason for at least indirect government involvement in Internet governance has to do with heightening awareness of Internet issues through the tools of education and information. Despite their soaring popularity, the Internet and electronic commerce are perplexing and intimidating to many people. The government's aim is to help eliminate barriers to full involvement in the Internet culture — by explaining the issues, pointing to the pitfalls and offering information that will help Canadians make better decisions.

Despite its continuing efforts to lend support, the Government of Canada wishes to see private-sector groups become even more extensively involved in the debates on reform and governance. This is not a mere matter of principle. Commercial, educational and other non-governmental groups have a lot at stake in these debates, and can explain and promote their own interests better than policy-makers and public officials. This is a particularly important consideration in the context of international consultations, given the very limited role for government in the creation of the new corporation. But private-sector involvement is also crucial at this stage because business people and anyone with an interest in electronic commerce will have a much better chance of identifying emerging commercial opportunities if they take the trouble to understand this new playing field and help to shape the ground rules that will define it.

GLOSSARY OF TECHNICAL TERMS

.ca - Canada's country code Top Level Domain (ccTLD).

.com - The generic Top Level Domain (gTLD) reserved for commercial entities.

.edu - The generic Top Level Domain (gTLD) reserved for universities and four-year colleges.

.gov - The generic Top Level Domain (gTLD) reserved for U.S. Federal government agencies.

.int - The generic Top Level Domain (gTLD) for organizations established by international treaties, or international databases.

.mil - The generic Top Level Domain (gTLD) used by the U.S. military.

.net - The generic Top Level Domain (gTLD) intended for organizations that administer or provide network connection services.

.org - The generic Top Level Domain (gTLD) used by many non-governmental organizations and other associations.

.us - The country code Top Level Domain (ccTLD) for the United States.

Address space - The aggregation of all possible IP numerical addresses assigned to hosts on the Internet.

Alternative dispute resolution - The process of using mediation, arbitration or negotiation to resolve a dispute instead of using the court system.

AlterNIC - Alternative Network Information Center. A generic Top Level Domain registry operating outside the IANA system.

APNIC - Asia/Pacific Network Information Center. The not-for-profit regional organization that allocates and registers IP address blocks in the Asia and Pacific Rim region (also see ARIN and RIPE).

ARIN - American Registry for Internet Numbers. The not-for-profit regional organization that allocates and registers IP address blocks for North America, South America, the Caribbean and sub-Saharan Africa (also see APNIC and RIPE).

ARPANET - The network created by the U.S. Department of Defense Advanced Research Projects Agency that preceded the Internet.

Bookmark - A method of storing the Internet address of a Web page so that the user can go to that address without having to re-enter it manually.

CAIP - Canadian Association of Internet Providers. An association of ISPs that addresses issues of industry-wide concern through collective and cooperative action.

ccTLD - country code Top Level Domain. The Top Level Domain that corresponds to each country's ISO 3166 code (e.g. .au for Australia, .ca for Canada).

CDNCC - Canadian Domain Name Consultative Committee. The organization responsible for creating a self-financing, not-for-profit corporation that will manage the .ca name space.

CIRA - Canadian Internet Registration Authority. The organization proposed by the Canadian Domain Name Consultative Committee (CDNCC) to manage the .ca name space.

CIX - Commercial Internet Exchange Association. An association of ISPs that seeks to develop consensus positions on legal and policy issues of mutual interest.

CORE - Council of Registrars. An IAHC-proposed consortium of private domain name registrars that would operate seven new gTLDs on a non-exclusive basis.

DARPA - Defense Advanced Research Projects Agency. The U.S. agency responsible for the development of ARPANET.

DISA - Defense Information Systems Agency. The organization that manages and protects the U.S. military's information infrastructure.

DNS - Domain Name System. A globally distributed database that translates domain names into numeric Internet addresses and vice versa.

Domain Name - The unique name that identifies an Internet site (e.g. www.yourbusiness.ca).

E-commerce - See Electronic Commerce.

eDNS - Enhanced Domain Name System. A generic Top Level Domain registry that operates outside the IANA system.

Electronic Commerce - Buying and selling goods and services over the Internet.

Green paper - "A Proposal To Improve Technical Management of Internet Names and Addresses (Discussion Draft)," issued by the NTIA on January 30, 1998. The initial U.S. government proposal for DNS reform that invited commentary from interested parties.

gTLD - Generic Top Level Domain names. The group of TLDs that includes .com, .org, .net., .edu, .mil, .int, .gov (see individual entries).

Host - A device in a network that accepts and transmits data. Examples include computers, printers, servers, terminals.

IAB - Internet Architecture Board. An organization that collects Internet-related research and participates in the development and technical evolution of the Internet, including its architecture and protocols.

IAHC - International Ad Hoc Committee. A coalition of participants from the Internet community, working to reform the DNS. It released its gTLD Memorandum of Understanding (MoU) on February 28, 1997.

IANA - Internet Assigned Numbers Authority. IANA allocates IP address blocks to the regional IP registries (ARIN, RIPE, APNIC) .

IETF - Internet Engineering Task Force. A component of the IAB responsible for developing Internet standards for review by the IAB.

IFWP - International Forum on the White Paper. An ad hoc coalition of Internet stakeholder groups organizing meetings internationally to discuss the U.S. White Paper on DNS reform.

InterNIC - Internet Network Information Center. The organization that provides domain name registration services for the top level domains .com, .net, .org and .edu. It comprises two distinct services partially funded by the NSF: Directory and Databases Services managed by AT&T and Registration Services managed by Network Solutions, Inc.

Interim board - The board that will determine the process by which the permanent governing board of the new corporation (see below) will be established, as well as its mandate and procedures.

Internet Address - Numerical 32-bit addresses expressed as four numbers between 0 and 255 separated by periods (e.g. 198.41.0.52) used to identify hosts that are connected to the Internet.

IP - Internet Protocol. The software rules that enable hosts to exchange data packets over the Internet.

IP address blocks - See IP number blocks.

IP number blocks - Internet addresses organized into blocks and assigned by IANA to regional IP registries.

IP number - The numerical address (e.g. 128.121.4.5) of each host on the Internet which is associated with a domain name (e.g. www.yourbusiness.ca) through the DNS.

IPv4 - The current version of the Internet Protocol which uses 32-bit addressing technology.

IPv6 - The 128-bit IP addressing technology proposed to succeed IPv4.

ISP - Internet service provider. An organization that provides users with access to the Internet. Sometimes called Internet access provider (IAP).

New corporation - The U.S.-proposed private not-for-profit organization that would oversee the DNS.

NSF - National Science Foundation. Provides support and grants for research in networking and communication, including the NSFNET and InterNIC.

NSFNET - National Science Foundation Network. A network funded by the National Science Foundation that formed part of what was to become the Internet.

NSI - Network Solutions, Inc. The exclusive registry for the .com, .net, .org and .edu domains.

NTIA - National Telecommunications and Information Administration. The agency of the U.S. Department of Commerce that advises the Executive Branch on domestic and international telecommunications and information technology issues.

Portals - Web sites that aggregate a large number and variety of content and services in order to attract visitors.

Protocol - A set of rules governing how data are to be transmitted and received over a computer network.

Registrant - One who applies for an SLD from a registrar.

Registrar - An organization authorized to enter and modify the SLD data maintained by a registry, in response to requests from registrants.

Registry - The organization that assigns, maintains and administers all services related to a TLD and its registrars.

RIPE - Réseaux IP Européens. The not-for-profit regional organization that allocates and registers IP addresses within Europe (also see ARIN and APNIC).

Root server system - The database used to match domain names to their equivalent numerical addresses in order to route data on the Internet.

SLD - Second Level Domain. That portion of the domain name that appears immediately to the left of the top level domain. For example, the "yourbusiness" in www.yourbusiness.ca.

TLD - Top Level Domain. That portion of the domain name that appears furthest to the right. For example, the .ca in www.yourbusiness.ca.

Trade-mark - A word, symbol, design, or combination of these, used to distinguish the wares or services of one person or organization from those of others in the marketplace. Trade-marks come to represent not only actual wares and services, but the reputation of the producer. As such, they are considered valuable intellectual property.

W3C - World Wide Web Consortium. The body that creates standards for the World Wide Web.

White Paper - The policy statement on DNS reform, entitled "Management of Internet Names and Addresses," issued by the U.S. Department of Commerce on June 5, 1998.

WIPO - World Intellectual Property Organization. The intergovernmental organization based in Geneva responsible for the advancement of intellectual property protection internationally, and the administration of multilateral treaties on intellectual property.

WWW - World Wide Web. An Internet application that links specially formatted files on host computers around the globe by means of the Hypertext Transfer Protocol (HTTP). This system allows users to retrieve text and multimedia information in a non-sequential way by clicking on links (known as URLs or uniform resource locators), and to download it through a browser like Netscape Navigator.