

## Government Regulation of the Dot-ca Domain Name Space

Marc Watkins\*

LONG GONE ARE THE DAYS when the Internet's Domain-Name System could be administered by a few computer and network scientists acting as self-appointed or matter-of-fact trustees of what was then a military research project funded by the U.S. Government. With the Internet becoming a commercialized communications network for the masses, resources and responsibilities for the Internet's key function of naming and addressing servers around the world had to shift from private individuals or university departments to new organisations dedicated to the task of allocating and managing domain names. During this transition the new organisations became more and more aware of the powers they inherited. Naturally, one did not have to wait long for national governments to take a stand on the issues involved. While there seems to exist an abundance of legal opinion in regard to the Internet Corporation of Assigned Names and Numbers, the U.S.-based guardian of the Internet's (official) name space, relatively little attention has been paid to the question of regulation by national governments when it comes to "their" country code Top-Level Domains. This article tries to help fill the gap by taking a closer look at the Canadian dot-ca Top-Level Domain-Name and the Canadian Government's current and possibly future regulatory regime. Emphasis is put on answering four key questions: What can be regulated? How can it be regulated? What is the current situation in Canada? And should there be regulation in the first place?

NOUS SOMMES BIEN LOIN de l'époque où le système des noms de domaine Internet était géré au moyen de quelques ordinateurs par quelques scientifiques de réseau, en tant que simples fiduciaires autodésignés de ce qui était alors un projet de recherche militaire financé par le gouvernement américain. L'Internet étant devenu un réseau commercial de communications de masse, nécessairement les ressources et les responsabilités en matière des fonctions Internet clés de la désignation et de l'accès aux serveurs partout dans le monde sont passés des individus privés et des départements universitaires à de nouveaux organismes spécialisés dans l'attribution et la gestion des noms de domaine. Durant la transition, ces nouveaux organismes ont pris peu à peu conscience des pouvoirs dont ils héritaient. Très rapidement, bien sûr, les gouvernements nationaux sont intervenus afin de se prononcer sur les questions en jeu. Bien qu'il semble y avoir une abondance d'opinions juridiques concernant la Société pour l'attribution des noms de domaine et numéros sur Internet, la gardienne (officielle) de l'espace des noms Internet établie aux États-Unis, très peu d'attention a été accordée à la réglementation par les gouvernements nationaux des domaines de premier niveau relativement aux codes de pays. Cet article tente de combler ce vide en explorant de plus près les noms de domaine canadiens de premier niveau point-ca et le régime canadien de réglementation, actuel et futur. L'article cherche à répondre à quatre grandes questions : Qu'est-ce qu'on peut réglementer? Comment peut-on réglementer ces questions? Quel est l'état actuel des choses au Canada? Et la réglementation est-elle de mise en premier lieu?

---

Copyright © 2005 by Marc Watkins.

\* Marc Watkins, University of Cologne, 1998; University of Ottawa, LL.M (concentration in Law and Technology), 2003. He was called to the German Bar in 2003 and works as an attorney for the law firm of Peters-Herrdum in Erkrath near Düsseldorf, Germany.

<b>147</b>	INTRODUCTION
<b>148</b>	1. ARCHITECTURAL POLICY RESTRICTIONS: WHAT CAN BE REGULATED?
<b>149</b>	1.1. <i>The Basic Technical Structure of the Domain Name System</i>
<b>151</b>	1.2. <i>The Delegation of Country Code Top Level Domain Names by ICANN</i>
<b>152</b>	1.2.1. RFC 1591 and ICP-1
<b>154</b>	1.2.2. The GAC Principles
<b>155</b>	1.2.3. New Country Code Name Supporting Organization (ccNSO)
<b>155</b>	1.2.4. Contracts between ICANN and ccTLD managers
<b>156</b>	2. INSTRUMENTS OF REGULATION: HOW CAN REGULATION BE EFFECTED?
<b>156</b>	2.1. <i>Administration of the Domain-name Space through Government Agencies</i>
<b>157</b>	2.2. <i>Legislation</i>
<b>157</b>	2.3. <i>Contracts</i>
<b>158</b>	3. THE SITUATION IN CANADA: WHAT IS REGULATED?
<b>161</b>	4. POSSIBLE REASONS FOR GOVERNMENT INTERVENTION: WHY REGULATE?
<b>162</b>	4.1. <i>The ccTLD as a National Resource</i>
<b>164</b>	4.2. <i>The ccTLD as a Public Resource</i>
<b>166</b>	4.3. <i>Proper Operation of .ca Name Servers</i>
<b>167</b>	4.4. <i>Equal Access to Domain Names</i>
<b>168</b>	4.5. <i>Fair Dispute Resolution</i>
<b>169</b>	4.6. <i>Accountability</i>
<b>172</b>	5. CONCLUSION

# Government Regulation of the Dot-ca Domain Name Space

Marc Watkins

## INTRODUCTION

MANY CANADIANS ARE BEGINNING to realize that, in addition to registering “.com” domain names, which until recently was a virtual *conditio sine qua non* for any serious website owner in North America, they also have the increasingly popular alternative of registering a domain name under “.ca,” Canada’s “country code Top Level Domain.” Over the last few years, .ca registrations have risen considerably and currently stand at around 493,000.<sup>1</sup>

Furthermore, country code Top Level Domains are playing an increasingly important role in the ongoing debate about international-domain-name governance as states begin to realize the role of the domain-name system as a means of controlling internet communication and of claiming “their” territory in the seemingly borderless realm of cyberspace. Therefore, country code Top Level Domains seem predestined to appear sooner or later on national governments’ regulatory radar, if they have not done so already.

This paper begins by outlining the constraints that the Canadian government—and for that matter any government in the world—faces when it attempts to regulate the Domain Name System, which is trans-national by nature; the first part of this paper therefore concerns “what can be regulated.” As will be seen, these constraints result from a mix of the architectural conditions of the current worldwide domain-name system as well as the regulatory regime governing the delegation of country code Top Level Domains which is set by the Internet Association for Assigned Names and Numbers (“ICANN”), the domain-name system’s primary administrative body. The second part of this paper provides an overview of three different ways for governments to influence the administration of their respective country code Top Level Domains: direct administration, legislation and contracts; this part concerns “how regulation can be

---

1. “Dot-ca Growth Strong,” *Canadian Internet Registration Authority* (February 2005), <<http://www.cira.ca/en/home.html>>.

effected.” The third part of the paper describes the system under which the .ca domain-name space is currently administered and the role that the Canadian government plays; this part concerns “what is regulated.” This paper restricts itself to an outline of the regulations directly aimed at the administration of the .ca domain-name space and excludes general legislation such as trademark law, which might also be applicable but which is not yet used by the Canadian government as a way to specifically set policies with regard to domain names.

The last part of this paper examines different possible justifications for policies of government intervention, stressing that the onus is on the government to show that more regulation is warranted; this part is therefore concerned with the possible justifications for regulation. It will be argued that arguments in favour of government regulation are at best weak and that, in particular, the technical set-up of the international Domain Name System, at least as it is currently in place, provides a sufficient degree of accountable self-regulation.

\*

## 1. ARCHITECTURAL POLICY RESTRICTIONS: WHAT CAN BE REGULATED?

IN THE CONTEXT OF COUNTRY CODE Top Level Domains,<sup>2</sup> it is important to determine the extent to which national governments are able to regulate at all. As a basic principle, national governments can only regulate to the extent that they can enforce any rules that they might impose.<sup>3</sup> Thus, based on the territorial concept of sovereignty, national regulatory power extends to and ends at the physical border to a sovereign neighbour.<sup>4</sup> Sometimes a national government’s exclusive power to regulate within its own borders is curbed by international treaties and conventions to which it must adhere. In the case of the internet’s Domain Name System (“DNS”), the power to regulate is further diminished by the technical architecture of the internet and the administrative structure behind it.<sup>5</sup> This part of the paper will explain the restrictions that national governments in general, and the Canadian government in particular, face when undertaking to regulate “their” ccTLD. Of special interest in this context is the triangular relationship between ICANN, the Canadian Internet Registration System (“CIRA”) and the Canadian federal government.<sup>6</sup>

- 
2. Forthwith, the common abbreviation “ccTLD” for the term “country code Top Level Domain” will be used.
  3. Henry H. Perritt, Jr., “Towards a Hybrid Regulatory Scheme for the Internet” (2001) U. Chicago Legal F. 215 at p. 249 and p. 256.
  4. David R. Johnson & David Post, “Law And Borders—The Rise of Law in Cyberspace” (1996) 48 Stan. L. Rev. 1367 at p. 1368, <[http://www.cli.org/X0025\\_LBFIN.html](http://www.cli.org/X0025_LBFIN.html)>; Catherine T. Struve & R. Polk Wagner, “Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act” (2002) 17 Berkeley Tech. L.J. 989 at p. 1024, <[http://www.law.berkeley.edu/journals/btlj/articles/vol17/STRUVE\\_WAGNER.pdf](http://www.law.berkeley.edu/journals/btlj/articles/vol17/STRUVE_WAGNER.pdf)>; Aron Mefford, “Lex Informatica: Foundations of Law on the Internet” (1997) 5 Ind. J. Global Leg. Stud. 211 at p. 214.
  5. The concept of software code and hardware architectures as a new means of regulation and as a restriction to traditional means of regulation is notably described by Lawrence Lessig in *Code and other Laws of Cyberspace* (New York: Basic Books, 1999).
  6. See Kenneth Neil Cukier, “Eminent Domain: Initial Policy Perspectives on Nationalizing Country-Code Internet Addresses” (June, 2002), <<http://www.cukier.com/inet02.html>> at III, arguing that the “triangular relationship” between ICANN, governments and ccTLD managers is a misnomer.

### 1.1. The Basic Technical Structure of the Domain Name System

This paper is not the place to provide an in-depth analysis of the technical functioning of the DNS,<sup>7</sup> but, in order to fully understand the interdependencies of the entities involved in administering the DNS, some basic facts have to be conveyed.

The DNS plays a vital role in the coordination of internet communication.<sup>8</sup> It translates user-friendly, alpha-numeric domain names into IP addresses, which are used by computers connected to the internet to identify each other and thereby make data transfers possible. If, for example, a user requests a web page by typing a domain name into a browser's address field, the browser will first contact a domain-name server, which is in most cases operated by the Internet Service Provider ("ISP") providing the internet connection. The name server then tries to match the domain name with a corresponding IP address, using its own locally stored domain-name database. If the domain name cannot be resolved because it is not stored in the cache, the name server tries to ask other name servers for the information.

Each domain name should have at least two name servers assigned to authoritatively carry the corresponding IP address information.<sup>9</sup> In order to find these name servers for the domain name in question, a database of all name servers for all domains under a Top Level Domain ("TLD") is maintained.<sup>10</sup> This database, called the "zone file," is maintained by the registries of the TLD in question. In the case of the ccTLD ".ca," this registry is CIRA.<sup>11</sup> CIRA's servers are the authoritative source of information for finding an IP address corresponding to a .ca domain name.<sup>12</sup>

However, CIRA does not occupy the top level in the hierarchy.<sup>13</sup> As an integral part of internet communication, the Domain Name System is internationally standardized and hierarchical.<sup>14</sup> Without this standardization and hierarchical structure, internet communication based on the DNS would not be

- 
7. For a more detailed explanation, see Ellen Rony & Peter Rony, *The Domain Name Handbook: High Stakes and Strategies in Cyberspace* (Lawrence, Kan.: R&D Books, 1998), <<http://www.domainhandbook.com/toc.html>>; Milton L. Mueller, "Technology and Institutional Innovation: Internet Domain Names" (2000) 5 Int'l J. Comm. L. & Pol'y. 1, <[http://www.ijclp.org/5\\_2000/pdf/ijclp\\_webdoc\\_1\\_5\\_2000.pdf](http://www.ijclp.org/5_2000/pdf/ijclp_webdoc_1_5_2000.pdf)>; Gregory R. Hagen & Kim G. von Arx, "The Patriation of .ca" (2002) 1 C.J.L.T. 79, <[http://cjlt.dal.ca/vol1\\_no3/pdfarticles/hagenarx.pdf](http://cjlt.dal.ca/vol1_no3/pdfarticles/hagenarx.pdf)> at p. 80.
  8. Jonathan Zittrain, "ICANN: Between the Public and the Private—Comments Before Congress" (1999) 14 Berkeley Tech. L.J. 1071, <<http://www.law.berkeley.edu/journals/btlj/articles/vol14/Zittrain/html/reader.html>> at p. 1073; for an account of what can happen if the Domain Name System is disrupted, see Rony & Rony, *supra* note 7 at p. 59.
  9. RFC 2182, s. 5, even recommends three or more independent DNS servers, R. Elz, et al., "Selection and Operation of Secondary DNS Servers" (1997) The Internet Engineering Task Force, <<http://www.ietf.org/rfc/rfc2182.txt>>. This is so for redundancy purposes. If the primary server fails to answer, the secondary (tertiary etc.) server provides backup, keeping the domain name available in case of failure of the primary server.
  10. Rony & Rony, *supra* note 7 at p. 62.
  11. See <<http://www.cira.ca>>.
  12. For a closer view of the general querying process within the DNS, see Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, Mass.: The MIT Press, 2002) at p. 41; ICANN, Internet Coordination Policy 3 (ICP-3), "A Unique, Authoritative Root for the DNS" (July 9, 2001), <<http://www.icann.org/icp/icp-3.htm>> [ICANN ICP-3].
  13. Rony & Rony, *supra* note 7 at p. 60.
  14. *Ibid.*; ICANN ICP-3, *supra* note 12; Mueller, *supra* note 12 at p. 41.

possible.<sup>15</sup> In order to make .ca domain names and other TLDs, such as .com, .org and so on, available worldwide and across the internet, the DNS has to specify where to find the authoritative servers for these domains. This task is conducted by the Root Server A and its 12 sister servers located around the world.<sup>16</sup> Root Server A is operated by ICANN.<sup>17</sup> The database maintained by these Root Servers, the “root zone file,” contains authoritative information on where to find the servers that maintain the databases for their respective domains.

It is important to emphasize that ICANN’s authority is primarily based on user convention.<sup>18</sup> While ICANN assumed its current function through a contract with the US government to take over the administration of the DNS,<sup>19</sup> the regulatory authority that ICANN enjoys is a simple consequence of the fact that the vast majority of name servers around the world acknowledge ICANN’s Root Servers as the ultimate technical authority for the lookup of domain names.<sup>20</sup> The Root Servers are at the top of the hierarchy and determine which name servers are responsible for the translation of a domain name into an IP address.<sup>21</sup>

The nature of ICANN’s authority based on user convention makes the DNS a rather unique example of a system governed by a standard-setting body. Given the fact that today’s internet communication largely relies on the proper functioning of the DNS, the hierarchical structure of the system and the widespread adherence to the authority of ICANN give the existing system—with ICANN on top—a huge advantage over alternative systems.<sup>22</sup> But all it would take to topple ICANN and replace it with a different entity or system is a concerted and coordinated re-routing of DNS lookup queries and some relatively minor changes in zone files and name-server software.<sup>23</sup> Moreover, individual users already have the ability to set their software applications to not use the

- 
15. Tamar Frankel, “The Managing Lawmaker in Cyberspace: A Power Model” (2002) 27 *Brook. J. Int’l L.* 859 at p. 871, <[http://www.brooklaw.edu/students/journals/bjil/bjil27iii\\_frankel.pdf](http://www.brooklaw.edu/students/journals/bjil/bjil27iii_frankel.pdf)>.
  16. While all 13 root servers are operationally on the apex of the DNS pyramid, Root Server A is first among equals because all other Root Servers derive their data from the authoritative Root Server A; see Peter K. Yu, “The Origins of ccTLD Lawmaking” (2003), <<http://www.peteryu.com/cctld.pdf>> at p. 2.
  17. For more Information on ICANN see <<http://www.icann.org>>, <<http://www.icannwatch.org>> and <<http://www.iana.org>>.
  18. In reality, the user’s ISP makes the decision to use ICANN as the authoritative root “on behalf” of the user, since the typical user is not interested in technicalities but mainly in one thing: connectivity.
  19. Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, <<http://www.icann.org/general/icann-mou-25nov98.htm>>; Hagen & von Arx, *supra* note 7 at p. 82.
  20. Kim G. von Arx & Gregory R. Hagen, “Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control” (2002) 9 *Rich. J. L. & Tech.* 4 at para. 77, <<http://law.richmond.edu/jolt/v9i1/Article4.html>>; *Supra* note 16 at p. 11; See also Mueller, *supra* note 12 at p. 53.
  21. Rony & Rony, *supra* note 7 at p. 516.
  22. Such systems exist but have not been, to date, overly successful; <<http://www.new.net>> offers alternative domain names that are not recognized by ICANN. See also <<http://www.opennic.unrated.net>> and <<http://www.open-rsc.org>>. See also ICANN ICP-3, *supra* note 12.
  23. Jonathan Weinberg, “ICANN and the Problem of Legitimacy” (2000) 50 *Duke L.J.* 187, <<http://www.law.duke.edu/journals/dlj/articles/dlj50p187.htm>> at p. 215; see Hagen & von Arx, *supra* note 7, for an analysis of the interesting idea that Canada should assume control over the “national” DNS by requiring domestic ISPs to map their servers to a governmental root server, thereby bypassing ICANN; See also Struve & Wagner, *supra* note 4 at p. 1023.

name servers within the “traditional” Domain Name System, but to point towards alternative Domain Name Systems.<sup>24</sup>

ICANN is powerful because nearly all name servers and software applications around the world “listen” to ICANN’s Root Servers.<sup>25</sup> Given the fact that the facilitation of connectivity provided by the Domain Name System is a valuable good which would be severely harmed if there were to be competing but incompatible Domain Name Systems,<sup>26</sup> any uncoordinated changes in ICANN’s position or in the role of the Root Servers are likely to fail, unless a mode of user-choice coordination can be found and efforts to educate users on how to exercise their choices get under way on a larger scale.<sup>27</sup>

### 1.2. *The Delegation of Country Code Top Level Domain Names by ICANN*

The role of ICANN as the authoritative and coordinating entity managing the Root Servers that decide which domain name is resolved by which name server makes it clear that each Registry responsible for the administration of its section of the DNS operates “at the mercy” of ICANN.<sup>28</sup> All TLD names are technically the same, whether they are generic names such as .com, .net, .org, etc., or whether they are ccTLDs such as .ca, .de, .uk, etc. CIRA, as the Registry maintaining the authoritative name servers for all .ca domain names, is no exception. If ICANN were to decide to re-delegate the administration of the .ca domain-name space to a Canadian entity other than CIRA, or even to a non-Canadian entity outside of Canada, all that it would have to do would be to alter the zone file entry for the .ca domain and to update the Root Servers.<sup>29</sup> Without internet users knowing, and without CIRA or the Canadian government being able to technically prevent it, ICANN could “pull the plug” on CIRA and “re-plug” elsewhere—anywhere around the globe.<sup>30</sup>

- 
24. Weinberg, *supra* note 23 at pp. 198–199. Users can either download software that reconfigures the internet connection accordingly (see <[http://www.new.net/help\\_faqs.tp](http://www.new.net/help_faqs.tp)>) or, subject to the user’s computer knowledge, can set the parameters manually (see <<http://support.open-rsc.org>> and <<http://www.opennic.unrated.net/personal.html>>).
  25. This power is not only of a technical nature, but it also forms the basis for ICANN’s exertion of regulatory power; see Struve & Wagner, *supra* note 4 at p. 1021. Furthermore, even some expressly alternative root server operators simply mirror ICANN’s root zone files, see <<http://european.orxn.net/faq.php>>.
  26. *Ibid.* at p. 1034. However, Cukier, *supra* note 6 at V, argues that, despite some possible problems with network reliability, the emergence of a splintered internet should not be seen negatively but rather as a reflection of “the natural diversity [...] that exists in the real world.”
  27. Frankel, *supra* note 15 at p. 868; Mueller, *supra* note 12 at pp. 50–56, argues that switching over to alternative roots is not a problem of technology but of coordination. He further speaks of the egg-and-chicken problem of alternative roots based on the economic principles of standards competition and network externalities: if only a few people use alternative roots, these roots are not attractive to others, especially if these roots are non-inclusive of the *de facto* standard represented by the “regular” ICANN DNS; see also Hagen & von Arx, *supra* note 7 at p. 88 and Yu, *supra* note 16 at p. 11, who argue that governments could combine their efforts and set up alternative roots or a new DNS if ICANN’s policies become overbearing.
  28. Von Arx & Hagen, *supra* note 20 at para. 46. Frankel, *supra* note 15 at pp. 870–872, likens the DNS to a “feudal structure” with ICANN as the “king.”
  29. Due to server caching, the changes would not be felt instantly across the internet, but under the current architecture the changes would automatically disseminate within days; see Mueller, *supra* note 12 at p. 49.
  30. See Hagen & von Arx, *supra* note 7 at p. 84, for an account of two “hostile re-delegations”; *in praxi*, this re-delegation would not take place smoothly unless ICANN had a backup zone file for the .ca domain that is not too outdated. However, even without such a backup a switch would be possible.

It becomes clear that any regulation of the .ca domain-name space by the Canadian government, and in fact all regulation with respect to the DNS, has to take into account the fact that the very subject of such regulation is not exclusively within the grasp of national governments, but is, on the contrary, very much embedded in the architecture of the internet itself and is placed into the hands of the entity that the users, and especially the ISPs and network administrators (*i.e.* the name-server operators), agree upon as being the standard-setting authority.<sup>31</sup> The leeway for regulation of the .ca domain-name space is limited by both technical restrictions and by ICANN's power to set delegation policies, as discussed below.

That having been said, ccTLDs are nevertheless different from generic TLDs—not because of a technical difference, but because of the way that the people involved in the early administration of the internet have set them up as domain-name spaces which are dedicated and delegated to the different countries and their citizens.

### 1.2.1. RFC 1591 and ICP-1

A key document reflecting this approach is RFC 1591.<sup>32</sup> The author of RFC 1591, Jon Postel, saw the need for setting guidelines for the delegation of ccTLDs to a capable designated manager adhering to the principles set out in RFC 1591.<sup>33</sup> While RFCs are not legally binding documents, they serve as widely accepted standards agreed upon by the technical internet community and set technical specifications and guidelines for the administration of the internet.<sup>34</sup>

The principles of delegating a ccTLD as set out in RFC 1591 are designed to ensure that the designated manager of the ccTLD is able to carry out the necessary tasks and has “the ability to do an equitable, just, honest, and competent job.”<sup>35</sup> Furthermore, the “designated authorities are trustees for the delegated domain, and have a duty to serve the community.” In addition, the designated manager is “the trustee of the top-level domain for both the nation,

31. Frankel, *supra* note 15 at p. 868.

32. RFC stands for “Request For Comments,” but effectively RFCs are *de facto* internet standards. For a more comprehensive description of the RFC system see RFC Editor *et al.*, “30 Years of RFCs” (1990), <<http://www.ietf.org/rfc/rfc2555.txt>>; additional information on RFC 1591 is available at Jon Postel, “Domain Name System Structure and Delegation” (1994), <<http://www.ietf.org/rfc/rfc1591.txt>> [RFC 1591].

33. RFC 1591 is supplemented by ICANN's “Internet Coordination Policy—1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)” (May 1999), <<http://www.icann.org/icp/icp-1.htm>> and by an IANA document outlining the ccTLD re-delegation procedure: “ccTLD Redellegation Step-by-Step Overview,” <<http://www.iana.org/cctld/redelegation-overview-19jun02.htm>>. Further documents relating to ccTLD governance include “ICANN Yokohama Meeting Topic: ccTLD Delegation and Administration Policies” (July 5, 2000), <<http://www.icann.org/yokohama/cctld-topic.htm>>; Paul Twomey, “Letter from GAC Chairman Paul Twomey Transmitting GAC Views on ccTLD Delegation and Administration Principles” (February 23, 2000), <<http://www.icann.org/committees/gac/twomey-letter-23feb00.htm>>; and “March 2000 ICANN Meeting in Cairo: ccTLD Delegation and Administration Policies” (March 2002), <<http://www.icann.org/cairo2000/cctld-topic.htm>>.

34. Zittrain, *supra* note 8 at p. 1078. For more information on the workings of RFCs see S. Bradner, “The Internet Standards Process—Revision 3” (October 1996), <<http://www.ietf.org/rfc/rfc2026.txt>>.

35. RFC 1591, *supra* note 32 at p. 4.

in the case of a country code, and the global internet community."<sup>36</sup> This shows that ccTLDs have a strong connection to the specific country or territory to which they are assigned.<sup>37</sup>

Important principles set out in RFC 1591 include those of consent and of the preservation of the status quo.<sup>38</sup> ICANN (as the successor of IANA<sup>39</sup>) only (re-)delegates the administration of a ccTLD if all "significantly interested parties in the domain should agree"; otherwise, it will leave things as they are.<sup>40</sup> However, there is an important exception to this principle: ICANN retains the right to step in if the proper administration of the domain is not secured.<sup>41</sup> Basically, it lies within ICANN's power to re-delegate the domain name to another managing entity if this action is in the interest of the proper operation of the DNS as defined by ICANN and if there are no direct remedies against such a decision.<sup>42</sup> Thus, RFC 1591 restates what ICANN, from a technical perspective, can do anyway—that is, to "unplug" CIRA if necessary.

RFC 1591 is complemented by another ICANN document: the Internet Coordination Policy 1 (ICP-1) "Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)."<sup>43</sup> Following the delegation principles laid out in RFC 1591, ICP-1 specifies policies of ccTLD administration and delegation. ICP-1 requires ccTLD managers to administer the ccTLD in an equitable manner and to treat "all groups in the domain" that request the registration of a domain name fairly and equally.<sup>44</sup> Furthermore, the manager must have the operational capacity and technical competence to fulfil the duties of a ccTLD Registry and, in particular, the duty to operate the database with accuracy, robustness and resilience and to otherwise cooperate with ICANN on technical questions.<sup>45</sup>

An important policy statement of ICP-1 is that ICANN, through IANA, will make the desires of the government of the country corresponding to a ccTLD a major consideration in all transfer or delegation proceedings with regard to a ccTLD.<sup>46</sup> This means that under ICP-1 governments have a significantly stronger position in the process of deciding who will administer that country's ccTLD than under RFC 1591 alone. This policy opens a direct way to influence ICANN/IANA as opposed to the indirect influence through participation in the Governmental Advisory Committee, which is discussed below. While ICANN still reserves the right to deviate from the government's "desires," especially when the desig-

---

36. *Ibid.* at p. 4.

37. The country codes correspond with the two-letter codes as set out in ISO standard 3166, <<http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html>>.

38. RFC 1591, *supra* note 32, s. 4 at p. 5.

39. "Internet Assigned Numbers Authority"; at the time of writing of RFC 1591 it was operated by Jon Postel himself.

40. RFC 1591, *supra* note 32, s. 4 at p. 5 and s. 6 at p. 6.

41. *Ibid.*, s. 5 at p. 6.

42. M. Stuart Lynn, "President's Report: ICANN—The Case for Reform" (February 24, 2002), <<http://www.icann.org/general/lynn-reform-proposal-24feb02.htm>>.

43. ICANN ICP-1, *supra* note 33.

44. *Ibid.* at p. 2.

45. *Ibid.*

46. *Ibid.*

nated ccTLD Registry violates other policy objectives like operational stability or fair and equitable treatment of registrants, the government's prerogative seems strong: unless a violation of ICANN's policies by the Registry is apparent, ICANN is likely to comply with the wishes of the government in question.

### 1.2.2. The GAC Principles

Within ICANN's multifaceted structure exist numerous committees,<sup>47</sup> one of which is the Governmental Advisory Committee, or "GAC."<sup>48</sup> It consists of representatives of national governments and is the main venue for input from those national governments wanting to get involved in ICANN's policy-making processes.<sup>49</sup> While the GAC is not restricted to involvement in the administration of ccTLDs, the policies surrounding the delegation of ccTLDs are certainly focal points for the GAC's activities.

Based on the principles of RFC 1591, in February 2000 the GAC issued the *Principles for the Delegation and Administration of ccTLDs Presented by Governmental Advisory Committee*.<sup>50</sup> It reiterates the statements made by Jon Postel: the designated manager—that is, the ccTLD Registry—is a trustee for the delegated domain and has a duty to serve the residents of the associated country as well as the global internet community.<sup>51</sup> But, other than RFC 1591, the GAC Principles also strengthen the position of national governments by stating that the designated manager "should recognize that ultimate public policy authority over the relevant ccTLD rests with the relevant government or public authority,"<sup>52</sup> which is a clear step towards government involvement in the administration of ccTLDs, as is also reflected by ICP-1. The GAC Principles even impose guidelines for the relationship between the designated manager of a ccTLD and the relevant government and ask for a copy of the communications between them to be forwarded to ICANN.<sup>53</sup>

The GAC Principles set rules for ICANN, the designated manager and the relevant government, and thus recognize and address the triangular relationship that exists between these players in the administration of ccTLDs. Nevertheless, it has to be kept in mind that those principles, like RFC 1591 or ICP-1, do not form a legally binding document. The authority of this document mainly derives from the fact that ICANN has the technical ability to re-delegate the .ca domain to other entities willing to abide by its rules.

---

47. See <<http://www.icann.org/committees/>>.

48. See ICANN Bylaw, *Bylaws for Internet Corporation for Assigned Names and Numbers* (October 13, 2003), Article XI, s. 2.1, <<http://www.icann.org/general/bylaws.htm#XI>>, for a description of the GAC's mandate.

49. The current representative for Canada is Malcolm Andrew, Industry Canada, <<http://194.78.218.67/web/contact/rep/index.shtml>>.

50. "Principles for Delegation and Administration of ccTLDs Presented by Governmental Advisory Committee" (February 23, 2000), <<http://www.icann.org/committees/gac/gac-ccldprinciples-23feb00.htm>> [GAC Principles].

51. RFC 1591, *supra* note 32 at p. 4.

52. GAC Principles, *supra* note 50 at s. 4.4.

53. *Ibid.* at s. 9.1.

54. See <<http://ccnso.icann.org>>.

### 1.2.3. New Country Code Name Supporting Organization (ccNSO)

ICANN is in the process of creating a new committee, called the Country Code Name Supporting Organization (“ccNSO”), which will consist of representatives of the ccTLD Registries—that is, of the designated managers.<sup>54</sup> Having the GAC as an opportunity for input from national governments, ICANN hopes to obtain the ccTLD Registries’ input through participation in the ccNSO. Core responsibilities of this committee will be the development and recommendation of global policies relating to ccTLDs and the fostering of consensus among the ccTLD Registry community and of general cooperation with other committees within ICANN.<sup>55</sup> It can be expected that the ccNSO will become an important venue with regard to ccTLD policies, and it will be interesting to see to what extent the ccNSO will compete with the GAC for the attention of ICANN’s board—especially if the ccNSO will be comprised of ccTLD Registries that are subject to very different degrees of government regulation and control. Should the ccNSO be controlled by ccTLD Registries who, in turn, are heavily controlled and regulated by their respective national governments, the ccNSO could be no more than a second GAC. However, should the ccNSO be controlled by Registries that are largely independent from their respective national governments, the power of influencing ccTLD policies would shift further away from those governments.

### 1.2.4. Contracts between ICANN and ccTLD managers

ICANN shows increasing desire to put its relation with ccTLD managers on a contractual basis. To this end it has created two model contracts: one that applies to a “legacy situation”<sup>56</sup>—i.e. when a ccTLD is delegated to a Registry without contractual involvement of a governmental authority—and one that applies to a “triangular situation”<sup>57</sup>—i.e. when a ccTLD is delegated to a Registry with the formal approval of the respective government. Currently, such agreements exist between ICANN and the Registries in Japan<sup>58</sup> (Japan Registry Service Co., Ltd.<sup>59</sup> or “JPRS”), Australia<sup>60</sup> (.au Domain Administration Limited<sup>61</sup> or “auDA”), Taiwan<sup>62</sup> (Taiwan Network Information Center<sup>63</sup> or “TWNIC”) and a few other ccTLD managers.<sup>64</sup>

These contracts have so far not been overly popular with ccTLD Registries. Only a handful have actually entered into contracts,<sup>65</sup> even though the

55. ICANN Bylaws, *supra* note 48 at Article IX, s. 1, <<http://www.icann.org/general/bylaws.htm#IX>>.

56. “Model ICANN-ccTLD Manager Memorandum of Understanding—Legacy Situation” (March 23, 2002), <<http://www.icann.org/cctlds/model-legacy-mou-23mar02.htm>>.

57. “Model ccTLD Sponsorship Agreement—Triangular Situation” (January 31, 2002) <<http://www.icann.org/cctlds/model-tsca-31jan02.htm>>.

58. “.jp ccTLD Sponsorship Agreement” (April 1, 2002) <<http://www.icann.org/cctlds/jp/>>.

59. JPRS website, <<http://jprs.jp/en/>>.

60. “.au ccTLD Sponsorship Agreement” (October 25, 2001), <<http://www.icann.org/cctlds/au/>>.

61. auDA website, <<http://www.auda.org.au/>>.

62. “.tw ccTLD Sponsorship Agreement” (March 26, 2003), <<http://www.icann.org/cctlds/tw/>>.

63. TWNIC website, <<http://www.twNIC.net/English/Index.htm>>.

64. For an overview, see <<http://www.icann.org/cctlds/agreements.html>>.

65. Interestingly, the agreements with the .jp, .au and .tw Registries were reached in connection with a re-delegation of the respective ccTLDs; see “IANA Report on Request for Redefinition of the .jp Top-Level Domain” (February 2002), <<http://www.iana.org/reports/jp-report-08feb02.htm>>; “Second IANA Report on Request for Redefinition of the .au Top-Level Domain” (November 19, 2001), <<http://www.iana.org/reports/au-report-19nov01.htm>>; and “IANA Report on Redefinition of the .tw Top-Level Domain” (May 29, 2003), <<http://www.iana.org/reports/tw-report-29may03.htm>>.

model contracts have been in existence for a few years. ccTLD Registries seem to be content with the non-contractual *status quo*, possibly because they feel that by entering into legally binding contracts with ICANN they would lose some of their regulatory autonomy and would subject themselves even more to ICANN's policy-making processes than is currently the case.

Governments also seem reluctant with respect to ICANN's ccTLD contracts. This is obvious for countries that already have more or less extensively regulated their domain-name space. Countries with domain-name legislation will be even more likely to have qualms about entering into contracts with ICANN or even about letting their Registries enter into one for fear of creating two competing regulatory regimes with respect to their ccTLD. Interestingly, even the "triangular" contracts that do exist between ICANN and the Australian, Japanese and Taiwanese Registries are not signed by the respective governments, notwithstanding the fact that those governments officially approved "their" Registry and its contractual relationship with ICANN.

\*

## 2. INSTRUMENTS OF REGULATION: HOW CAN REGULATION BE EFFECTED?

BEFORE REVIEWING THE REGULATORY SITUATION in Canada, it is helpful to provide a summary of some forms of regulation that can be envisioned by governments intending to influence or set domain-name policies.

### 2.1. Administration of the Domain-name Space through Government Agencies

The most direct way of influence is the administration of the ccTLD through an agency that is part of or under the direct control of the government. A recent example is Ireland, where the administration of the ".ie" domain-name space currently lies with a non-profit organization,<sup>66</sup> but will be transferred over to the Commission for Communications Regulation,<sup>67</sup> the statutory body responsible for the regulation of the electronic-communications sector in Ireland.<sup>68</sup> In Finland, the administration of the ".fi" domain-name space is vested in the Finnish Communications Regulatory Authority (FICORA).<sup>69</sup>

Under this model, the government usually has full control over the staff that administers the domain-name space and owns or otherwise directly controls the necessary hardware. A disadvantage of this regulatory option could become evident when the administration lies with an agency without its own legal personality since this agency would not be able to enter into a contract with ICANN, if it so desired. In this case, any contract would have to be between ICANN and the government or state itself.

---

66. IE Domain Registry Ltd, <<http://www.domainregistry.ie>>.

67. ComReg, <<http://www.comreg.ie>>.

68. ITU Strategy and Policy Unit Newslog (April 20, 2004), <<http://www.itu.int/osg/spu/newslog/categories/europe/2004/04/20.html>>; Breaking News.ie, "Comreg take over control of domain name," <<http://www.breakingnews.ie/2004/04/13/story142644.html>>.

69. FICORA website, <<http://www.ficora.fi/englanti/index.html>>.

Administration of a ccTLD through a government agency is often supplemented by corresponding legislation, which is another obvious way for states to regulate.

## 2.2. Legislation

Some countries, such as Spain,<sup>70</sup> Finland,<sup>71</sup> South Africa<sup>72</sup> and Ireland,<sup>73</sup> have opted for regulating their domain-name space, at least partially, through legislation. Legislation in the area of domain-name administration can have two regulatory objectives. First, legislation may determine who will administer the ccTLD in question. It may subsequently also prescribe the Registry's organizational structure and its rights and obligations.<sup>74</sup> Second, legislation itself can set certain policy directives with respect to registration, revocation, dispute resolution and so on, leaving only executive tasks for the Registry.<sup>75</sup>

In so far as such legislation designates a certain Registry as the responsible entity for domain-name administration, it is in essence unnecessary since it is ultimately ICANN that delegates the domain-name administration and not national governments. The value of legislation can only be seen in the formal affirmation of ICANN's choice by the national legislature and thus has only declaratory meaning within the existing regime of RFC 1591, ICP-1 and the GAC Principles. Legislation might bind the national Registry but it does not bind ICANN and, therefore, the reasons for legislation are considerably narrowed down.

Another problem is the impact of "special" legislation for the Registry on the existing general laws and regulations of a nation. When regulating the dispute-resolution process regarding domain names, for example, it has to be kept in mind that such regulation has an impact on many other areas of law, most notably trademark law, fair-trade laws and even private international law.<sup>76</sup> Legislating the operations of a Registry or setting specific policies for domain-name registrations may entail the danger of inconsistencies with existing laws.

## 2.3. Contracts

Another regulatory option for governments would be to contractually bind the Registry into meeting certain policy objectives that the government imposes. In

70. The Spanish ccTLD.es is operated by a state company and registrations of .es domain names are regulated through a host of governmental decrees. For further details, see the cctldinfo website's information on Spain, <<http://www.cctldinfo.com/country.htm#es>>.

71. *Finnish Domain Name Act 2003*, <[http://www.ficora.fi/englanti/document/Domain\\_Name\\_Act.pdf](http://www.ficora.fi/englanti/document/Domain_Name_Act.pdf)>.

72. B8-2002, *South African Electronic Communications and Transactions Bill, 2002* <<http://www.gov.za/gazette/bills/2002/b8-02.pdf>>.

73. *Electronic Commerce (Ireland) Act 2000*, Article 31, <<http://www.dcmnr.gov.ie/files/comms%20reg%20electronic%20commerce%20act%202000.pdf>>.

74. *Finnish Domain Name Act 2003*, *supra* note 71, s. 17.

75. See sections 4 to 12 of the *Finnish Domain Name Act 2003*, *supra* note 71, setting exact policies and procedures for the registration and termination of a domain name under the .fi ccTLD.

76. Laeffer speaks of domain names as a hybrid form of intellectual property; see Marshall Laeffer, "Sovereignty and the Globalization of Intellectual Property: Domain Names, Globalization and Internet Governance" (1998) 6 *Ind. J. Global Legal Stud.* 139 at p. 145. This underlines the notion that domain-name regulation should be made consistent with a variety of existing "offline" legal frameworks and should not represent an isolated legal regime.

Canada, this contractual approach to regulation is so far only manifested in the general terms of the Umbrella Agreement between the University of British Columbia ("UBC"), CIRA and Industry Canada, which will be laid out in the next part of the paper. Under this agreement, CIRA is obliged to meet the policy goals that may be set by the Canadian government, or otherwise the latter can terminate the contract and the delegation.

The problem arising again is that such contracts between national governments and ccTLD Registries are not legally binding on ICANN and therefore the regulatory value of these contracts is diminished by the delegation principles imposed by ICANN. Another difficulty is the state's limited capacity to regulate by contract. In the case of ICANN's contractual relationship with the US government it is argued that, if ICANN makes public policy in, *inter alia*, the realm of dispute resolution and trademark law, governments may not outsource this public policy-making power to a private non-profit organization (which also executes its own decisions) and may not regulate this organization through contracts without any further publicly legitimized supervision.<sup>77</sup>

The question of the state's ability to regulate ccTLDs by contract largely relates to the accountability problem, which will be discussed in more detail later,<sup>78</sup> and thus the same arguments apply. In particular, the notion that domain-name policy constitutes public policy falling within the scope of administrative law, which is critical to Froomkin's and Weinberg's arguments, will be examined.<sup>79</sup>

Rather than enter into a contract with the Registry, a different option for governments would be to force the Registry to enter into a contractual relationship with ICANN. As stated above, ICANN is eager to develop these contractual relationships with ccTLD Registries and provides model contracts that have already been used in relation to several ccTLD Registries. However, this option might prove inadequate for countries that already have a strong regulatory regime and possibly even legislation in place. As mentioned above, governments of countries like Finland or Ireland that administer their ccTLD through a government agency are unlikely to replace or even just restrict their own system by means of a contract with ICANN. In addition, the governments of countries in which a more or less independent Registry administers the domain-name space are likely to think twice before permitting a contract between the Registry and ICANN to set a legal status quo that might prove difficult to change later on and thus restrict the government's own regulatory power.

★

### 3. THE SITUATION IN CANADA: WHAT IS REGULATED?

THE ABOVE-MENTIONED POLICY documents restrict Canada's ability to regulate the .ca domain-name space autonomously. The Canadian government has to

---

77. A. Michael Froomkin, "Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Consitution" (2000) 50 Duke L. J. 17 at 184, <<http://www.law.miami.edu/~froomkin/articles/icann.pdf>>; Weinberg, *supra* note 23 at p. 219.

78. See below, part 4.6.

79. See below, part 4.2.

always keep in mind ICANN's requirements for proper domain-name administration when making policy decisions. However, the government is not left without any means to influence the ICANN part of the regulatory equation. Firstly, there is the GAC to which Industry Canada sends a representative.<sup>80</sup> Through the GAC processes within ICANN, Canada can try to influence decisions and to initiate new policies. On the other hand, Canada has only one voice among many in a committee that is itself only one of many committees involved in ICANN's decision-making process.<sup>81</sup> Secondly, the Canadian government can attempt to lobby ICANN and to build on the principles set out in RFC 1591, and especially on the GAC Principles, which give governments a say in how ccTLDs should be administered. Thirdly, the Canadian government can address the United States government and thereby try to exert influence over ICANN indirectly. The US government is in a strong position in relation to ICANN because ICANN is a non-profit organization which is incorporated in the US and which operates by virtue of a contract with the US government.<sup>82</sup>

Even with restrictions in place, government regulation is still possible within the boundaries set by ICANN's policies. A number of countries have used their remaining regulatory power to put in place legislation or to set up government agencies to administer their respective ccTLDs.<sup>83</sup> The majority of countries have left the administration to either commercial or non-profit organizations, and then have formalized their relationship with these organizations through, for instance, a contract or have opted not to formalize the relationship.<sup>84</sup>

This is also the path that the Canadian government took with respect to the .ca ccTLD. CIRA is a not-for-profit organization and, yet, it has formalized ties with the government.<sup>85</sup> Before CIRA's incorporation, the administration of the .ca domain-name space was conducted by John Demco of the University of British Columbia.<sup>86</sup> He individually assigned and registered domain names to applicants upon request and at his own discretion.<sup>87</sup> As the internet became more popular and demand for domain names grew, this system was no longer sufficient.<sup>88</sup> After negotiations between the Canadian government, UBC, the Internet Society Canada and other stakeholders, a consensus was established around the incorporation of CIRA. This decision was formalized in the Umbrella Agreement that regulated the transition of domain-name administration from the UBC system to

---

80. *Supra* note 49.

81. For an overview of ICANN's committee structure, see <<http://www.icann.org/general/icann-org-chart.htm>>.

82. Hagen & von Arx, *supra* note 7 at p. 82. See also Struve & Wagner, *supra* note 4.

83. See <<http://www.cctldinfo.com/overview.html#government>> at Table 1 for a list of countries.

84. *Ibid.*

85. There is no official documentation as to why a private, not-for-profit organization was chosen. For an analysis of possible reasons see Timothy Denton, "Canadian Domain Name Governance: The Twice Delegated CIRA" (November 29, 2000) at p. 17, <[http://www.tmdenton.com/pub/presentations/cdn\\_domain\\_governance.pdf](http://www.tmdenton.com/pub/presentations/cdn_domain_governance.pdf)>.

86. *Ibid.* at 3.

87. Hagen & von Arx, *supra* note 7 at p. 83; Canadian Domain Name Consultative Committee, "Framework for the administration of the .CA domain name system" (September 15, 1998), <[http://www.cira.ca/official-doc/12.CDNCC\\_Final\\_Report.pdf](http://www.cira.ca/official-doc/12.CDNCC_Final_Report.pdf)>.

88. Canadian Domain Name Consultative Committee, *ibid.*

CIRA's system.<sup>89</sup> Besides regulating the transition, the relationship between CIRA and the Canadian government is also laid out in this agreement. Furthermore, Michael Binder of Industry Canada wrote a letter to ICANN stating that CIRA was the new designated ccTLD Registry for Canada.<sup>90</sup> This letter aimed at corroborating CIRA's "legitimacy" with respect to ICANN's decision to re-delegate the .ca ccTLD from the UBC to a better-equipped entity. In another letter to CIRA, Michael Binder set out policy goals for CIRA which are widely identical to the policy goals prescribed under the Umbrella Agreement.<sup>91</sup>

The Umbrella Agreement states that "CIRA shall manage, operate and control ... the .ca domain space in accordance with the principles and structure set out in the March 11 Letter and in accordance with other principles as CANADA may, from time to time, set."<sup>92</sup> An important provision can be found in paragraph four of the Umbrella Agreement: The Canadian government may terminate the designation of CIRA if, in the opinion of the Canadian government, CIRA is unable to continue to manage, operate and control the .ca domain space in accordance with the principles set out by the Canadian government.

However, currently there exist no official policy documents or directives by the Canadian government other than the general principles set out in the Umbrella Agreement and the Binder Letters. This fact leads to the conclusion that to date there was no reason for the Canadian government to intervene in the operations of CIRA and that CIRA's policies and regulations are in line with the government's views. In that respect it might even be argued that the .ca domain-name space is so far not regulated at all by the Canadian government. The mere availability of the means of coercion—which could ultimately terminate the delegation—without imposing any substantive policy directives on CIRA other than mandating the proper and equitable operation of the .ca domain-name space does not amount to regulation, unless one already views tacit approval as a form of regulation.

To complete the picture of governmental ways to control CIRA it should be mentioned that the Canadian government has the right to have a representative sit on CIRA's Board of Directors as a non-voting ex-officio member.<sup>93</sup> As this representative has no voting rights, his or her function is largely restricted to gaining access to information within CIRA's organization. On the other hand, even this seemingly passive form of participation in the decision-making process of CIRA can be a valuable tool for the Canadian government to influence CIRA's policies. Having a person on the inside gives the government the opportunity to "lobby" the voting members of CIRA's board and to be heard before policies are actually put into force, making it possible that many decisions are influenced by

---

89. *Umbrella Agreement for the Transfer of the .ca Domain Name Registry Between University of British Columbia and Canadian Internet Registration Authority and Her Majesty the Queen in Right of Canada*, <[http://www.cira.ca/official-doc/31.umbrella\\_agreement.pdf](http://www.cira.ca/official-doc/31.umbrella_agreement.pdf)>, [Umbrella Agreement].

90. Letter from Michael Binder (Industry Canada) to Michael Roberts (ICANN) (October 10, 2000), <<http://www.iana.org/reports/industry-canada-letter-10oct00.htm>>.

91. Letter from Michael Binder (Industry Canada) to Robert Hall (CIRA) (March 11, 1999), <<http://www.iana.org/reports/industry-canada-letter-11mar99.htm>>.

92. Umbrella Agreement, *supra* note 89.

93. CIRA By-Law No. 1 (July 7, 2003), s. 3.01(b)(ii), <<http://www.cira.ca/en/agm/doc/Bylaw1-20030625-en.pdf>>.

the government's views without formal or public action.

Finally, it should be pointed out that CIRA, as all legal entities with rights and obligations, is bound by the existing general laws. It has to follow the legislative policies formulated in acts and regulations and has to follow court decisions. The operation of the .ca domain-name space is influenced by trademark law and by privacy law; CIRA itself is influenced by corporate law, contract law and other laws. However, these influences of general laws are not within the scope of this paper. To date, legislative action has not been a way to regulate CIRA or the .ca domain-name space directly and as such.<sup>94</sup>

\*

#### 4. POSSIBLE REASONS FOR GOVERNMENT INTERVENTION: WHY REGULATE?

HAVING OUTLINED THE RESTRICTIONS for government regulation in the field of ccTLD administration and having described the status quo of the delegation of the .ca domain-name space to CIRA, it is necessary to examine the need for further government regulation.

There are several approaches to arguing in favour of self-governance in the context of cyberspace and particularly domain names. First, there is the general view that, in a free society, governments should always refrain from regulation unless intervention becomes necessary, with cyberspace being no exception.<sup>95</sup> A variation of this general principle is represented by free-market theory in its numerous facets, but its application depends on whether the domain-name space can and should be seen as a market place.<sup>96</sup>

A different approach is what could be called the historically motivated argument in favour of self-governance, which contends that the internet emerged and prospered because it was unregulated and was only governed by its tech-savvy "cyber-citizens" through technical standards and self-imposed "netiquettes."<sup>97</sup> Regulation, especially government regulation, is seen as impeding the force that made the internet what it is today.

Another approach is propagated by scholars who not only say that the state should not regulate cyberspace, but also that the state is not even fully capable of regulating cyberspace due to its international and technological nature. In their view, cyberspace represents a new realm that is not subject to traditional territory-based government regulation.<sup>98</sup>

94. This is a contrast with the United States, whose controversial *Anticybersquatting Consumer Protection Act* directly regulates domain names.

95. Bertelsmann Foundation, "Who Controls the Internet? The Bertelsmann Foundation's Recommendations for Internet Governance" (2000), <<http://www.democratic-internet.de/berlin2001/recommendations.pdf>> at p. 43.

96. Frankel, *supra* note 15 at p. 861. She argues that ICANN controls a unique market place, applying a theory of contestable markets to its operation, *ibid.* at pp. 895–900.

97. Johnson & Post, *supra* note 4 at p. 1388; Bertelsmann Foundation, *supra* note 95 at pp. 38–40.

98. Most famous is John Perry Barlow's "A Declaration of the Independence of Cyberspace," <<http://www.eff.org/~barlow/Declaration-Final.html>>; see also Johnson & Post, *supra* note 4 at p. 1370 and 1378; see, explicitly with regard to domain names, Laeffer, *supra* note 76 at pp. 160–161.

This part of the paper is premised on a sceptical view towards government regulation. After starting each heading with an argument in favour of government regulation, it will be attempted to show that none of these arguments ultimately support demands for more government intervention. To be clear, this mode of argumentation is more or less an arbitrary choice and must not obscure the general principle that the onus should be on the government to establish the need for more regulation.

#### 4.1. The ccTLD as a National Resource

One of the reasons for government regulation of ccTLDs could be that, as they are an important national resource, they have to be under national control.<sup>99</sup>

This is what could be labelled the "sovereignty," "independence" or "proprietary" argument.<sup>100</sup> Given the fact that ccTLDs follow the ISO standard 3166 and are assigned to the corresponding country, they seem to constitute some kind of national property resource that, quite "naturally," should be subject to sovereign disposition.<sup>101</sup> As a consequence of being a national resource, ccTLDs allegedly have to be available to the citizens of the country.<sup>102</sup>

Although the people responsible for the administration of the early domain-name system stressed the non-political nature of their activities, the introduction of ccTLDs effectively gave countries their "own" part of the internet.<sup>103</sup> This approach is mirrored in the notion that a ccTLD is a country's "face on the internet." CIRA extensively markets the .ca domain as a Canadian resource. It touts itself as an organization that provides registration services "by Canadians for Canadians"<sup>104</sup> and that encourages Canadians to register .ca domains instead of other domain names, especially the popular .com domain, and underlines this encouragement with the slogan "Speak Canadian."<sup>105</sup> Another of CIRA's slogans is "Made in .CA Canada" and is the catchphrase for an Open Forum on "Canada's Internet Space."<sup>106</sup> The strongest indicator of the proprietary approach is CIRA's

99. Von Arx & Hagen, *supra* note 20 at paras. 22 and 64, citing ICANN's Governmental advisory committee; Michael Geist, "Governments and Country-Code Top Level Domains: A Global Survey" (December 2003), <<http://www.michaelgeist.ca/geistgovernmentcctlds.pdf>> at p. 2 and p. 5.
100. Geist, *ibid.*; Hagen & von Arx, *supra* note 7 at p. 79; von Arx & Hagen, *supra* note 20 at para. 64; Yu, *supra* note 16 at p. 10; Struve & Wagner, *supra* note 4 at p. 1027; Cukier, *supra* note 6 at I and V.
101. It has been found that 75% of Canadians believe that ".ca" means Canada and 90% believe that it is important to have the .ca ccTLD as a resource for Canadians; see Presentation by Allan Gregg to CIRA (December 6, 2001), "Canadian Attitudes Toward the Dot-ca Domain," <[http://www.cira.ca/official-doc/104.cira\\_tsc\\_en.pdf](http://www.cira.ca/official-doc/104.cira_tsc_en.pdf)>. See also Hagen & von Arx, *supra* note 7 at p. 89 (footnote 1); von Arx & Hagen, *supra* note 20 at para 22.
102. The equal-access requirement as a reason for government intervention is addressed separately below.
103. See RFC 1591, *supra* note 32 at p. 6, where Jon Postel emphasized that "the IANA is not in the business of deciding what is and what is not a country". However, the granting of a ccTLD to a country or territory can be viewed as "cyberspace recognition," as the case of the Palestinian TLD ".ps" shows; see Jonathan Blavin & Jeremy Kutner, "Global Ideal, National Reality" (2000), <<http://cyber.law.harvard.edu/icann/pressingissues2000/briefingbook/nationalism.html>>.
104. Denton, *supra* note 85 at p. 3; NOIE Case Study on Canada's .ca domain, <<http://www.noie.gov.au/projects/international/gac/news/caReDelegation.htm>>.
105. See CIRA trademarks, including "Speak Canadian," <[http://www.cira.ca/en/about\\_trademarks.html](http://www.cira.ca/en/about_trademarks.html)>.
106. See CIRA news release, "Made in .Canada: An Open Forum on Canada's Internet Space" (March 18, 2003), <<http://www.cira.ca/news-releases/95.html>>.

Canadian Presence Requirement Policy, which requires registrants of a domain name to be a Canadian citizen or permanent resident, a holder of a Canadian trademark, or some kind of entity with ties to Canada.<sup>107</sup>

While it is somewhat natural for CIRA and the Canadian government to understand the .ca domain-name space as a Canadian resource, the sovereignty and proprietary arguments face a number of counter-arguments. Firstly, there are numerous ccTLD Registries that allow not just citizens but in fact anybody to register domain names in their domain-name space.<sup>108</sup> Some of the largest and most popular ccTLDs follow this open approach; for example, Germany currently has 8.4 million registrations in its .de domain.<sup>109</sup> Additional examples include such countries as Tuvalu (.tv domain), Turkmenistan (.tm domain) and Western Samoa (.ws domain). Those countries market their domain names all over the world – or outsource this task or even “sell” the domain name altogether – because of their generic character; for instance, .tv appears to stand for “television,” .tm for “trademarks” and .ws for “website.”<sup>110</sup> This shows how ccTLDs do not necessarily have to be restricted to their corresponding country.

One could argue that the option to “sell out” the domain name does not deprive it of its national character. To this argument it could be conceded that the economic factor is not decisive. For example, in the case of Tuvalu, which sold its .tv domain name to a private company,<sup>111</sup> the proceeds benefit the citizens of the country in much the same way as the sale of land to foreigners does not necessarily lead to a loss of sovereignty over that land. But if the national character of a domain name is not lost by opening up the domain-name space to foreigners and not even by altering its meaning from a country denominator to a generic denominator, then the national character of a domain name bears little weight for arguing in favour of government regulation. For example, after selling its domain name to a foreign country, Tuvalu would have a weak argument if it were to attempt to justify government regulation by way of the “national” character of the domain name that it sold.

Countries like Canada, which do not sell their domain name space and do not allow registrations by non-residents, could argue that, while others may act differently, they preserve the national character of the ccTLD and thus do not lose it as a basis for government regulation. However, if it is a policy choice not to “sell out” the domain-name space, then it is—on its own merit—a weak argument namely because the justification for governmental policy-making should not depend on another governmental policy decision. In other words, if the national character of a domain name is founded on the positive choice of a gov-

107. See CIRA Policies, Procedures and Guidelines, “Canadian Presence Requirements For Registrants” (November 8, 2000), <[http://www.cira.ca/official-doc/18\\_1.RPPG\\_00006EN.pdf](http://www.cira.ca/official-doc/18_1.RPPG_00006EN.pdf)>.

108. About 70 countries do not have presence requirements for registering a domain under their ccTLD; see Blavin & Kutner, *supra* note 103.

109. See DeNIC, <[http://www.denic.de/en/faqs/domainanmelder/index.html#section\\_25](http://www.denic.de/en/faqs/domainanmelder/index.html#section_25)> and <<http://www.denic.de/en/domains/statistiken/index.html>>.

110. Yu, *supra* note 16 at p. 10. For additional examples of “repurposed” ccTLDs, see <<http://domains.dan.info/structure/countrycodes.html>>.

111. Tuvalu’s .tv domain is operated by The .tv Corporation International, a California-based company; see <<http://www.tv/en-def-687a07b2e6a1/en/index.shtml?accepts=en-us>>.

ernment to preserve this character, then this national character can hardly be a strong justification for government regulation. A true justification for an action should not depend on an autonomous choice—*i.e.* one that is not compelled by outside forces—that is made by the actor itself.

There are two further arguments against using the national character as a justification for government regulation. The first is that even ccTLDs are part of the international DNS.<sup>112</sup> While ccTLDs were specifically set aside for the corresponding countries, the delegation of ccTLDs does not change their technical character as an integral part of the DNS. Indeed, from a technological standpoint there is no difference at all between ccTLDs and generic TLDs;<sup>113</sup> both are part of the same global DNS.<sup>114</sup>

Another argument is even blunter but goes to the heart of the problem. Even if ccTLDs were to qualify as a national resource, why would this warrant government regulation? There are, at least in the context of domain names, no reasons for government regulation solely based on the national character of a matter. The fact that a resource is attributed to a specific country is not in itself a sufficient reason for government intervention as opposed to a private-sector initiative. This point is proven by successful ccTLDs such as the .de domain.<sup>115</sup> The German government does not regulate the administration of domain names through specific legislation nor through a specific policy—other than by condoning the actions taken by the .de Registry.<sup>116</sup>

Therefore, the national character of ccTLDs, even if one is ready to admit that it exists, is not in itself a justification for government regulation.

#### 4.2. *The ccTLD as a Public Resource*

Stressed even more often than their character as a national resource is the notion that ccTLDs are an important public resource.<sup>117</sup> Again, the examination of this argument has to be twofold. Is the premise of public character true and is the conclusion that government regulation is warranted correct? In addition, it has to be kept in mind that any argument for government regulation using the notion of “public resource” is to some extent circular. It is hard to define “public resource” without borrowing from murky concepts such as “the public interest” and it is hard to define public interest without borrowing from the notion of

112. In fact, RFC 1591 itself deals with TLDs—generic and country codes—in general and makes only additional provisions for ccTLDs where necessary.

113. Computers do not recognize the difference between generic TLDs and ccTLDs. Both are on the same level of the domain-name tree. For a more detailed account, see RFC 1034, <<http://www.ietf.org/rfc/rfc1034.txt>>.

114. Milton L. Mueller, “Internet Domain Names: Privatization Competition And Freedom Of Expression” (1997) Cato Institute Briefing Paper No. 33, <<http://www.cato.org/pubs/briefs/bp-033.html>> at para. 36, which puts it pointedly by saying that, “...national TLDs are nothing more than badly truncated, semantically unattractive generic TLDs.” See also Rony & Rony, *supra* note 7 at p. 46 (Figure 3.5), p. 60 (Figure 3.7) and p. 108 (Figure 4.5).

115. Germany's .de ccTLD is the largest in the world in terms of registrations (6.8 million in November 2003); see <<http://www.denic.de/en/domains/statistiken/index.html>>.

116. For further information on cctlinfo and Germany, see <<http://www.cctlinfo.com/country.htm#de>>.

117. See Letter from Binder, *supra* note 91; Umbrella Agreement, *supra* note 89, Preamble 3; Geist, *supra* note 99 at 2,6 and 8; Cukier, *supra* note 6 at l. Even Internet communication as a whole is sometimes declared a global public good; see Bertelsmann Foundation, *supra* note 95 at p. 32.

domain names as a public resource.

It could be argued that ccTLDs are a public resource because they are an integral and important part of internet communication, that internet communication is beneficial to economic and social development and that therefore domain names can be likened to public resources like roads or radio waves, both of which are subject to a wide range of government policies.<sup>118</sup> As shown above, the Domain Name System is indeed vital to all internet communication at present and for the foreseeable future.<sup>119</sup> Because of its importance, the proper functioning of the DNS as a whole is surely in the public interest, just as the proper maintenance of streets is in the public interest.

However, the communicational importance of the DNS cannot warrant government regulation with regard to ccTLDs. Firstly, ccTLDs—or any *specific* domain name—are not, in fact, vital for the operation of the DNS as a communications facilitator.<sup>120</sup> In principle, there would have to be only one (or a few) TLD(s) for the DNS to function.<sup>121</sup> From a technical standpoint, the proper operation of the .ca domain is not vital for internet communication as a whole. Domain names resemble telephone numbers in the sense that one needs a telephone number in order to receive phone calls, but it does not matter what that number is, as long as it works properly.<sup>122</sup> Admittedly, the .ca domain-name space is important for internet communication with computers making use of the .ca domain, but, even if the .ca domain were to cease to exist, users would migrate their websites to other domains. This argument cannot be dismissed on grounds that existing users of .ca domain names are entitled to use their old .ca domain name for their internet communications or that a country is “entitled” to have its own operational ccTLD.<sup>123</sup> From a technical standpoint, all domains are equally efficient. To declare special rights in terms of the use of .ca might be warranted from a “national-property” standpoint, but this exits the realm of the argument of a “public resource because of communicational importance” and goes back to ccTLDs as a national resource, which was dismissed earlier in this paper.

But even if one were to acknowledge a “right” to have a Canadian TLD in place and even if one were to recognize its value for Canadian economic and

118. See Mueller, *supra* note 12 at p. 218.

119. See Zittrain, *supra* note 8.

120. A single branch of the domain-name tree can be easily truncated without disrupting its functions as a whole. The only part that cannot be removed is the root of the tree. See Rony & Rony, *supra* note 7 at p. 60. It could be argued that even the root can be removed, but this would only be true for the specific computer hosting the root file. However, if this computer were taken offline, this would not eliminate the need for a root server as a technical necessity. Some other computer would take its place and become the new root. See Mueller, *supra* note 12 at p. 49.

121. Today there exist over 250 Top Level Domains. See Froomkin, *supra* note 77 at p. 43.

122. Of course, it has to be kept in mind that domain names are often more than cryptic addresses but are in fact meaningful monikers; see Rony & Rony, *supra* note 7 at p. 18. In this sense domain names resemble not only telephone numbers, but novelty phone numbers (“1-800-COLLECT”), which give it some further meaning. However, this additional functionality is not necessary for ensuring proper communication, be it domain names or telephone numbers.

123. Questions of entitlement to domain names are difficult to answer, both for individual Second Level Domains and for Top Level Domains. It would seem that countries do not have legal title to their existing ccTLD unless such a claim could be supported by international law or through a contract with ICANN. As for individual .ca Second Level Domains, an entitlement can be argued to exist through a registrant’s contract with CIRA regarding the domain name. Another possible source for entitlement could be trademark law. But even if such entitlements do exist, it can be argued that they do not guarantee the existence of domain names *per se* and *ad infinitum*.

social development, there is no need for government regulation to ensure its protection against interferences. Unlike radio waves, which must be regulated in order to avoid interference by “wild broadcasting,” the DNS is much more resilient against such interference because of its self-organizing tendency. This tendency is based on the character of the DNS as an agreed-upon, standardized system. The DNS works because everybody uses it.<sup>124</sup> Everybody uses it because every internet user wants to enjoy maximum connectivity, which in turn can only be achieved if everyone uses the same system.<sup>125</sup> Truly autonomous, alternative Domain Name Systems have failed to establish themselves.<sup>126</sup> The vast majority of ISPs set up their name servers and program their software to listen to the name servers administered by ICANN.

All this happens without government intervention and is driven by the need for global connectivity in combination with technical necessities such as unambiguous domain names.<sup>127</sup> Unlike with radio waves, there is no real danger of “chaotic interferences” in the DNS because either one is an integral part of it and one necessarily subordinates oneself to the given DNS hierarchy, or one uses a different system, loses connectivity to the other system and thereby excludes oneself automatically, without interference.<sup>128</sup> This (technical) self-regulating and self-organizing tendency of the DNS shows that .ca domain names cannot be likened to public roads or radio waves, whose users can indeed interfere with each other. Therefore, government intervention based on the need for coordination and protection against interference is not warranted.

#### 4.3. Proper Operation of .ca Name Servers

Given the importance of the DNS for internet communications, it could be argued that a failure to properly operate the name servers administering the .ca domain-name space, thereby causing loss of connectivity, would result in significant economic damage and that, therefore, the Canadian government has a responsibility to ensure or to at least supervise the proper maintenance of this critical infrastructure, just like it does with roads, airports, telephone networks and the broadcasting infrastructure.<sup>129</sup>

First of all, this argument is related to the argument that domain names are a public resource, which was criticized above, and therefore suffers from the same weaknesses. Secondly, as with all government intervention, the onus should be on the government to show that it has to step in and that matters can-

---

124. Froomkin, *supra* note 77 at p. 44 and p. 47.

125. Mark. A Lemley, “Antitrust and the Internet Standardization Problem” (1996) 28 Conn. L. Rev. 1041 at p. 1045.

126. See *supra* note 22.

127. *Supra* note 125 at p. 1046.

128. It could now be argued that this loss of interconnectivity on the internet is the same as interference in the case of radio waves: both make proper communications more difficult. But then the question arises as to whether it is the state’s responsibility to restore connectivity by way of regulation, even if it was the user’s own choice to use a different system.

129. This reasoning seems to underlie the Finnish *Domain Name Act 2003*, *supra* note 71. Section 1 reads: “The objective of this Act is to promote the provision of information society services in information networks....”

not be left as they are. The current operation of the name servers and of other infrastructure related to the administration of the .ca domain-name space by CIRA has shown no problems. Thirdly, ICANN's ccTLD delegation policies clearly indicate that the proper operation of the domain-name space is the primary task of the respective Registries and that ICANN will make sure that all the necessary requirements are met.<sup>130</sup> If a Registry fails to fulfil its basic responsibilities, ICANN will re-delegate the administration of the domain-name space in question to an entity more willing and more able to preserve connectivity.<sup>131</sup> Therefore, the supervision by ICANN should provide an incentive for CIRA to meet international standards and safeguards to the extent necessary to make government regulation in this field unnecessary.

#### 4.4. Equal Access to Domain Names

Another argument in favour of government intervention could be that only legislation can ensure equal access to domain names.<sup>132</sup> A particular characteristic of domain names is that their number is virtually unlimited,<sup>133</sup> but that only some are desirable because they make semantic sense (*i.e.* names, locations, abbreviations, generic words).<sup>134</sup> And while their number is unlimited, it is a technical necessity that there not be two identical domain names under the same Top Level Domain.<sup>135</sup> Also, given the fact that domain names are chosen to make semantic sense, they can conflict with "real-world" names and trademarks.<sup>136</sup> Therefore, the decision as to who can register which domain name is important and has to be made with a view to ensuring that everyone has equal access to domain names, especially if one views the administration of the .ca domain-name space through CIRA as a monopoly controlling access to an important (even if not public) resource.<sup>137</sup>

However, equal access to domain names is not an argument *per se* for government regulation. The uniqueness of any given domain name within the same DNS is a technical necessity. Given this technical premise, the most widely adopted registration principle put in place by registries around the world is the "first-come, first-served" principle, which is also implemented in CIRA's registra-

---

130. See RFC 1591, *supra* note 32 at p. 6.

131. *Ibid.*

132. See *supra* note 129, s. 1; Bertelsmann Foundation, *supra* note 95 at p. 32, for equal access to the internet in general.

133. For one TLD alone the number of possible Second Level Domains is, theoretically, at least 36 to the power of 22, given that domain names may comprise the 26 letters of the alphabet plus the numbers 0–9 and can be up to 22 characters long. Of course, this number increases with longer domain names. And then there are over 250 Top Level Domains. See *supra* note 121.

134. For a description of "namesmithing" and of marketing of domain names, see Rony & Rony, *supra* note 7 at pp. 24–28.

135. See Froomkin, *supra* note 77 at p. 41.

136. See Laeffer, *supra* note 76 at pp. 146–51. For a detailed account of early domain-name disputes, see Rony & Rony, *supra* note 7 at pp. 299–378.

137. For a discussion of the natural monopoly with respect to internet communication standards and US anti-trust law, see Lemley, *supra* note 125. Lemley, at p. 1062, points out that governments frequently regulate situations where natural network monopolies tend to arise, such telephone and broadcasting systems.

tion rules and procedures.<sup>138</sup> CIRA registers domain names to the first applicant unless it has positive knowledge that the applicant's registration would violate trademark rights or other rights of third parties.

In essence, the problem of ensuring equal access to .ca domain names is not so much a matter of the government regulating access but rather is more a matter of fair registration and of, in particular, fair dispute-resolution policies. While the need for a fair dispute-resolution process is separately addressed below, the whole complex of CIRA being an entity that sets and enforces policies with regard to domain names is a general problem of the public accountability of CIRA and of public control over its actions, which is also addressed below.

#### 4.5. Fair Dispute Resolution

Another potential argument in favour of government regulation of the domain-name space is the need to manage conflicts arising from the registration of domain names and the need to establish a fair dispute-resolution process.<sup>139</sup> Dispute resolution is at the heart of the intersection between domain-name policy and traditional legal regimes. This is especially true for trademark and trade-names law, the field most often touched by disputes over domain names. It could be argued that only governmental regulation of the resolution of such disputes can provide enough protection for trademarks and other important business interests. Just as the state provides for protection and dispute resolution in the bricks-and-mortar world, it must also protect those rights in the online environment.

The fair-dispute-resolution argument, however, is not as strong as it seems, partly because it carries one counter-argument already within it. The state, by providing dispute resolution in the "real world" also provides dispute resolution in the online environment.<sup>140</sup> There are only a few reasons why the conventional methods of resolving disputes through administrative processes or in the courts might not seem to be sufficient when it comes to domain names. Those reasons are the high costs of court proceedings and the great physical distances between the parties that are often encountered in such disputes because of the trans-national character of domain names. Online dispute resolution is a cheaper and more convenient way to deal with disputes. But these reasons do not warrant government regulation. The high costs of court proceedings are a problem that not only arises in domain-name disputes but in all kinds of disputes and are therefore a problem that states have to address generally and not because of the nature of domain-name disputes.<sup>141</sup>

---

138. See CIRA Policies, Rules and Procedures, Rule 2.9 of the Registration Rules, <<http://www.cira.ca/en/documents/q2/RegistrationRules-EffectiveDateJune52003.pdf>>.

139. This goes hand-in-hand with the need to protect intellectual-property rights in domain names, which is one of the main reasons for governments to regulate ccTLDs; see Geist, *supra* note 99 at p. 7; see also WIPO, "ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes" (June 2001), <[http://www.wipo.int/freepublications/en/e-commerce/839/wipo\\_pub\\_839.pdf](http://www.wipo.int/freepublications/en/e-commerce/839/wipo_pub_839.pdf)>.

140. See Mueller, *supra* note 114.

141. This argument is corroborated by looking at the German ccTLD, whose Registry DeNIC has no dispute-resolution policy in place; see DeNIC website domain name FAQs, <[http://www.denic.de/en/faqs/recht\\_dispute/index.html#section\\_99](http://www.denic.de/en/faqs/recht_dispute/index.html#section_99)>. Although the .de ccTLD is the largest by number of registrations and, consequently, there is a considerable number of domain-name disputes, the German government at present does not view the lack of a special dispute-resolution regime as an insufficiency and there are no plans to change the status quo of leaving domain-name disputes to the courts; see cctldinfo website information on Germany: <<http://www.cctldinfo.com/country.htm>>.

Besides the argument that the state already provides dispute-resolution mechanisms and that therefore there is no need for additional government involvement, another argument shows that government-provided mechanisms are not the right approach. This argument is associated with the above-mentioned character of the DNS as an extra-national system of user standards: given the fact that the administration of domain names is independent from geographical locations<sup>142</sup> and given the fact that it is also volatile because it purely consists of standards and software settings that have no “real-world” connection other than the physical name servers, it follows that it is not subject to direct state enforcement.<sup>143</sup> Unless states control the physical Root Servers, their respective governments have no means to delete or transfer a domain name other than by ordering the domain-name registry to make the necessary changes in software and server settings.<sup>144</sup>

Another factor that reduces policy options for governments with respect to domain-name dispute resolution and the enforcement of decisions is the already-mentioned strong influence of ICANN. While ICANN will to some extent respect the policy choices of governments regarding “their” ccTLDs, ICANN always has the option of imposing its own policies and, if the registry of the ccTLD does not comply, ICANN can always re-delegate the administration of the ccTLD.<sup>145</sup>

An additional argument against government regulation is that states would have to show that the current online-dispute-resolution system put in place by CIRA is insufficient. CIRA provides for an online arbitration process to solve disputes over domain names.<sup>146</sup> Since October 2002 over a dozen domain-name disputes have been decided under the CIRA dispute-resolution policy.<sup>147</sup> At this point, the dispute-resolution system seems to be working satisfactorily and is thus without need for government intervention or correction.

#### 4.6. Accountability

Another argument in favour of government regulation is that of accountability for the administration of the .ca domain-name space.<sup>148</sup> CIRA’s tasks do not end with the technical administration of domain names and with providing connectivity,

142. See Hagen & von Arx, *supra* note 7 at p. 80.

143. Froomkin calls the state’s control over the DNS “ephemeral”; see Froomkin, *supra* note 77 at p. 44.

144. See Hagen & von Arx, *supra* note 7 at p. 80. And even if states control the physical servers or effectively order the registry to make the necessary changes, the ccTLD zone file could be simply moved to other servers that are not under the influence of the state—for example, to servers in offshore jurisdictions. WIPO, *supra* note 139 at p. 8, recommends that ccTLD administrators should commit to directly implement decisions resulting from dispute-resolution procedures without further revision or confirmation by “regular” courts.

145. See RFC 1591, *supra* notes 40 and 41.

146. See CIRA Dispute Resolution Policy, <[http://www.cira.ca/official-doc/CDRP\\_Policy\\_2003-12-04\\_en\\_final.pdf](http://www.cira.ca/official-doc/CDRP_Policy_2003-12-04_en_final.pdf)>.

147. The full texts of the decisions are available at the CIRA website, <[http://www.cira.ca/en/cat\\_dpr\\_decisions.html](http://www.cira.ca/en/cat_dpr_decisions.html)>.

148. See Geist, *supra* note 99 at p. 6; Froomkin, *supra* note 77 at pp. 27–28, discussing the parallel situation regarding ICANN and the US Department of Commerce and the non-delegation doctrine regarding the exercise of public power; Perritt, Jr., *supra* note 3 at pp. 223–224, addressing the problem of accountability of private regulation of the internet; Weinberg, *supra* note 23 at p. 212, who, like Froomkin, discusses the parallel situation of ICANN and its legitimacy.

but they also include a lot of policy-making and the implementation of these policies in day-to-day operations. CIRA sets policies about who can register domain names,<sup>149</sup> which domain names can be registered and which cannot be registered,<sup>150</sup> what the procedure is for domain-name registrations<sup>151</sup> and which companies are certified as registrars acting as technical and contractual mediators between registrants and CIRA.<sup>152</sup> Most importantly, CIRA makes policies for the resolution of domain-name disputes and sets criteria for the deletion or transfer of a domain name in case of a dispute.<sup>153</sup> As a result of the proximity of domain-name disputes to trademark law, tort law and unfair trade practices, CIRA's policies in this field have a significant impact on these areas of law. This proximity could be seen as being reason enough to favour government regulation or supervision. The situation is exacerbated by the fact that CIRA is not only the policy-maker in this area but that it also has the sole power to execute decisions reached through the dispute-resolution process.<sup>154</sup> Thus, CIRA has both legislative and executive powers when it comes to the .ca domain-name space. It could be argued that CIRA has monopolized control over a popular resource and that only legislation, or at least governmental supervision, can democratically justify such a concentration of power. Furthermore, it could be argued that mechanisms must be put in place to challenge CIRA's policy-making and its execution of decisions in order to make CIRA publicly accountable for its actions.<sup>155</sup>

But even these seemingly strong arguments in favour of government regulation have considerable weaknesses. The public-accountability argument largely depends on the premise that the .ca ccTLD is a public resource, which was criticized earlier, and on the premise that policies for the administration of domain names are public policies.<sup>156</sup>

Another argument against the view that government regulation is needed in order to provide public accountability is based on the concept of the DNS as a system of user standards as described above. Every internet user can choose to use a different DNS than that which is operated by CIRA and ICANN and is free either to express dissent by switching systems or to acquiesce by staying with the existing system.<sup>157</sup> Some scholars argue that switching costs can be prohibitively high if switching means exclusion from the prevalent communica-

---

149. For a full overview of CIRA's policy documents, see <[http://www.cira.ca/en/cat\\_Registrar.html](http://www.cira.ca/en/cat_Registrar.html)>.

150. *Ibid.*

151. *Ibid.*

152. See CIRA's certification policies, <[http://www.cira.ca/en/cat\\_Registrar.html](http://www.cira.ca/en/cat_Registrar.html)>.

153. CIRA Dispute Resolution Policy, *supra* note 146.

154. CIRA makes policy by formulating its Registration Policies and Dispute Resolution Policies. Then it also executes the decisions reached pursuant to these policies by way of registering, deleting or reassigning domain names.

155. See Weinberg, *supra* note 23 at p. 216, describing the parallel situation with ICANN. He argues that ICANN has taken on tasks, such as the coordination of a vital communications resource, that were traditionally left to government bodies.

156. Weinberg, *ibid.* at p. 217, justifies the need for legitimizing ICANN by pointedly saying that "ICANN's exercise of control looked, walked and quacked like public regulatory power."

157. See Neil Weinstock Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory" (2000) 88 Calif. L. Rev. 395 at p. 425.

tion system.<sup>158</sup> This might diminish user choice to a degree where there is no alternative to the current system and thus no real choice remains.<sup>159</sup> But it is not clear whether switching costs are really that high<sup>160</sup> and also whether, if they are, this still warrants special government intervention. Firstly, there are other examples where freedom of choice is absent or diminished, but those cases are left to existing anti-trust laws.<sup>161</sup> Anti-trust laws might be applicable to the administration of domain names, which shows that further government regulation through instruments other than the existing general laws is not needed.<sup>162</sup> Secondly, even in industries that rely on a single standard, the setting of this standard can be left to market forces rather than to government intervention.<sup>163</sup> Thirdly, the cost of switching would not be high if there were to exist a system that facilitates the use of a workable alternative DNS or if internet users were technically educated to exercise their choices.<sup>164</sup> The current lack of such a facilitating system should not be a reason to establish government regulation instead of user choice. To do otherwise would amount to an uncalled-for substitution of the tacitly made policy choices of complacent non-voters (*i.e.* “non-switchers”) with the policy choices of the government. In other words, if there are anti-competitive barriers preventing users from exerting self-regulatory rights, it would seem to be the task of a liberal state to remove the barriers rather than to accept the barriers and to substitute self-regulation with governmental regulation.

There are further positive arguments in favour of self-regulation as a means of ensuring accountability. One advantage of self-regulation is congruence—that is, the idea that the people whose rights are directly affected should be the ones who have a say in the adoption of the rules.<sup>165</sup> This is the case when internet users make the choice of whether to adhere to the Domain Name System operated by CIRA/ICANN. All .ca domain-name registrants are by default a member of CIRA and elect the board members who then set the relevant policies.<sup>166</sup> Even “regular” internet users that are not domain registrants have the above-mentioned choice of redirecting their DNS lookups to other servers. Moreover, that most internet users do not opt out while being aware of the current policies can be seen as acquiescence, which may be seen as one way of establishing accountability.<sup>167</sup>

---

158. *Ibid.* at pp. 425–427 and pp. 436–437; Henry. H. Perritt, Jr., *supra* note 3 at p. 222.

159. *Supra* note 157 at p. 426.

160. Froomkin, *supra* note 77 at p. 42, identifies a mix of users’ lack of knowledge and inertia as the main reasons why switching does not take place on a larger scale.

161. One obvious example is the Microsoft’s market power. See Mark A. Lemley, *supra* note 125 at p. 1048; *Supra* note 157 at p. 441. Although Microsoft has a strong market position because of the fact that the market for operating systems tends to revolve around a dominant standard, all that is done is to apply general anti-trust laws. Nobody suggests that Microsoft should be turned into a government agency or be subject to special legislation.

162. Lemley, *supra* note 125 at p. 1079.

163. *Ibid.* at 1059. Lemley gives the example of the battle of VHS versus Betamax over home-video standards, which was resolved through market forces, albeit at the expense of Betamax users whose equipment became useless.

164. See *supra* note 160.

165. Perritt, *supra* note 3 at p. 312; Johnson & Post, *supra* note 4 at p. 1393.

166. See CIRA By-Law No. 1, *supra* note 93, s. 12.01.

167. Perritt, *supra* note 3 at p. 236.

\*

## CONCLUSION

WHEN CONSIDERING GOVERNMENTAL REGULATION of ccTLDs it has to be kept in mind that there exists a triangular relationship between ICANN on the international level and the government and CIRA on the national level. ICANN is the technical and administrative authority when it comes to the delegation of ccTLDs. Regulatory measures have to conform to the policies and principles put in place by ICANN in order to avoid re-delegation. While the Canadian government may be able to exert influence on ICANN to some extent, it is clearly restricted in the way that it is able regulate the administration of the .ca domain-name space.

Several arguments can be brought forward in favour of increased government regulation of CIRA and of the .ca domain-name space. Yet this paper argues that none of these arguments is really strong enough to warrant government regulation. Such arguments as the qualification of ccTLDs as national or public resources are weakened by examples of countries "selling out" their domain names and marketing them as generic names. While domain names are important for internet communication in general, specific domain names, such as .ca, are not. Therefore, they cannot be seen as a public resource. Another argument against government intervention is that there are already policies and procedures in place like the CIRA dispute-resolution process that deal with certain issues arising in the context of domain names.

Furthermore, government regulation cannot be justified on accountability grounds. Even if domain registries do in fact make public policies, the power to make such policies is a consequence of users allowing their computers to "listen" to their name servers and of users thereby assenting to the way that domain registries administer the name space. Given the fact that the infrastructure confers such a built-in freedom of choice, governments should allow the system to regulate itself and should abstain from imposing their own representative democracy over the existing grass-roots, democratic architecture of the DNS.

If the Canadian government were nevertheless to choose to regulate, it would face some further difficulties. Legislation can effectively only be passed within the boundaries already set by ICANN. Furthermore, as with many internet-related issues, government regulation of a particular phenomenon within cyberspace such as ccTLDs poses the problem of harmonizing this new and specific regulation with the existing general law. Contracts, as a different way of influencing CIRA in order to meet regulatory objectives, suffer from the same fault of not involving ICANN and of therefore facing restrictions set by ICANN's delegation policies. Furthermore, if one justifies contractual regulation with the argument that CIRA administers a public resource and makes public policy, then the question arises of whether such regulation can legally be delegated by entering into contracts without greater public accountability and control.