

ANTITRUST

INTERNET AND DOMAIN NAME GOVERNANCE: ANTITRUST LITIGATION AND ICANN

By Lily Blue

This Note examines the development of the Internet's governance structure from its rudimentary beginnings to its current complex regulation by the Internet Corporation of Assigned Names and Numbers (ICANN). The Note focuses on the difficulties facing ICANN, in particular the threat of antitrust litigation, by considering the merits of possible antitrust claims against ICANN as well as ICANN's pro-competitive justifications for its challenged practices. Ultimately, the Note concludes that how ICANN would fare under antitrust scrutiny depends largely on its ability to demonstrate that its policies serve the interests of the Internet community and do not restrict competition.

Part I of this Note briefly reviews the technologies supporting the Internet and its Domain Name System. Part II discusses the evolution of Internet governance from small, ad hoc management to complex, multi-layered governance. Part III considers the possibility that ICANN and its affiliated organizations might receive antitrust immunity in federal courts and therefore not be subject to antitrust litigation at all. Part III also examines in detail the substantive merits of the antitrust claims against ICANN while considering pro-competitive justifications that ICANN could present in defending itself against these allegations.¹

Finally, Part IV concludes the Note by reviewing challenges still facing Internet governance. These challenges may, in due course, require further changes to the Internet's governance structure.

I. OVERVIEW OF THE INTERNET AND THE DOMAIN NAME SYSTEM.

The Domain Name System (DNS) is a key element of the Internet governance system. Domain names are crucial to the livelihood of the Internet because they make Internet addresses easier to remember, thereby aiding communications and business transactions. Section A of this Part

© 2004 Berkeley Technology Law Journal & Berkeley Center for Law and Technology.

1. See *United States v. Microsoft*, 253 F.3d 34, 59 (D.C. Cir. 2001) (“[I]f a plaintiff successfully establishes a prima facie case under § 2 by demonstrating anticompetitive effect, then the monopolist may proffer a ‘pro-competitive justification’ for its conduct.”) (quoting *Eastman Kodak Co. v. Image Technical Servs., Inc.*, 504 U.S. 451, 483 (1992)).

briefly describes the technology involved in the DNS and the Internet. Section B discusses the structural organizations and processes involved in obtaining and using a domain name. Section C describes the different levels of domain name organization.

A. Technology

The Internet is a web of interconnected computers sharing standardized communication protocol software.² The standardized protocols allow a computer connected to the Internet to communicate with any other connected computer. Each computer is assigned a unique network address, a virtual location in cyberspace defined by an Internet protocol (IP) number.³ IP addresses are used to route information from one computer to another, and the IP itself forms the basis for more reliable, higher-level protocols.⁴

Because IP numbers are long, arbitrary, and nearly impossible to remember, Internet developers created the DNS, a database that replaces each IP number with alphanumeric codes called domain names.⁵ When an Internet user enters a domain name into a web browser, a computer database called a Domain Name Server translates the name into its corresponding IP number.

B. The Domain Name System and Its Regulating Bodies

The current DNS has a hierarchical structure.⁶ For example, *www.berkeley.edu* is a domain name comprised of a series of alphanumeric codes representing each domain level separated by periods.⁷ Within

2. See *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 849-50 (1997); see also 47 U.S.C. § 230(f) (2000) (defining the Internet as “the international computer network of both Federal and non-Federal interoperable packet switched data networks”).

3. See *Reno*, 521 U.S. at 844; see also ICANN, Glossary of Terms and Abbreviations, at <http://www.icann.org/general/glossary.htm> (last visited Mar. 8, 2004) (defining “Internet protocol”).

4. Ryan Owens, Note, *Domain-Name Resolution After Sallen v. Corinthians Licenciamentos & Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona*, 18 BERKELEY TECH. L.J. 257, 259 (2003).

5. *Id.*; see also 15 U.S.C. § 1127 (2000) (defining domain names as “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet”).

6. *Name.Space v. Network Solutions, Inc.*, 202 F.3d 573, 577 (2d Cir. 2002); see also ICANN, *Top-Level Domains*, at <http://www.icann.org/tlds> (last visited Nov. 25, 2003) [hereinafter ICANN, *Top-Level Domains*] (describing the tree-like hierarchy of the DNS).

7. See generally *Name.Space*, 202 F.3d at 573.

each domain name, the field to the far right is called the Top Level Domain (“TLD”), the next field to the left is called the Second Level Domain (“SLD”), and so on.⁸ The TLDs, like *.edu*, *.com*, and *.org*, are fixed; only ICANN can approve the creation of these domains.⁹ The SLDs, such as *.berkeley* in this example, can be registered by paying a registration fee to a registry, an entity that governs a particular TLD.¹⁰

Each registry regulates the files and servers that allow a specific TLD to function.¹¹ Registries do not directly register the SLDs available for the TLD it controls. Rather, registries merely publicize the SLDs available within each particular TLD they govern. ICANN, which is not a registry itself, oversees and governs the registries.¹²

Neither the registries nor ICANN have direct contact with customers (as registrants) interested in obtaining SLD names. Instead, other entities, known as registrars, aid customers in registering domain names. Registrars search a particular registry’s TLD to determine whether a customer’s requested SLD has already been taken. If the domain name is available, then the customer pays a registration fee to the registrar, usually for one or two years of registration. The registrant will then have exclusive control of the domain name.¹³

C. Categories of Top Level Domains

There are two types of TLDs. The first group, known as generic Top Level Domains (“gTLDs”), include the most well-known TLDs: *.com*, *.net*, *.org*, *.edu*, *.gov*, *.int*, and *.mil*.¹⁴ Anybody can register SLDs within the first three gTLDs (*.com*, *.net*, and *.org*),¹⁵ but only certain organizations and entities can register SLDs within the latter four (*.edu*, *.gov*, *.int*,

8. *Id.*

9. See ICANN, *Top-Level Domains*, *supra* note 6; see also *infra* Part I.C.

10. See *infra* Part I.B.

11. See generally Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, 2003 U. ILL. L. REV. 1, 7 (2003). Each TLD has a root file and a root server that contains databases enabling an Internet address query to be routed to its proper destination. See *Name.Space*, 202 F.3d at 577. That is, when an Internet user enters a query for a domain name (or a Second Level Domain) into the computer, the computer will route this query to the root file of the specific TLD in question. The root file will then search the particular TLD until the requested domain name is found and the website connected to. *Id.*

12. See generally Froomkin & Lemley, *supra* note 11.

13. *Id.* at 7.

14. ICANN, *Top-Level Domains*, *supra* note 6.

15. *Id.* Under the *.com*, *.net*, and *.org* gTLDs, anyone with an interest in obtaining a SLD could do so, although *.net* was supposedly created for networks, and *.org* was supposedly created for organizations.

and *.mil*).¹⁶ ICANN recently introduced seven new gTLDs.¹⁷ Four of these (*.biz*, *.info*, *.name*, and *.pro*) are open to the public, while the other three (*.aero*, *.coop*, and *.museum*) are limited to specific entities.¹⁸

The second type of TLDs is the country code Top Level Domains (“ccTLDs”) owned and operated by at least 45 different countries around the world.¹⁹ Unlike gTLDs, which serve populations without geographical limitations, ccTLDs are dedicated to serving different countries.²⁰ Consequently, ICANN does not maintain the ccTLDs; governments or affiliated institutions of each respective country control most of them.²¹ A few ccTLDs are maintained by independent individuals or academic institutions within these countries.²²

II. INTERNET GOVERNANCE

This Part examines the rudimentary beginnings of the Internet’s governance. It then discusses ICANN’s organizational structure and decision-

16. *Id.* Under *.edu*, only United States educational institutions can register domain names. *Id.* Under *.gov*, only the United States government entities may register domain names. *Id.* Under *.int*, only organizations established by international treaties between governments may register domain names. *Id.* Under *.mil*, only the United States military may register domain names. *Id.*

17. *Id.*

18. *See id.* Generally, an unsponsored gTLD operates under policies “established by the global Internet community directly through the ICANN process” while a sponsored gTLD is a specialized gTLD that has a sponsor representing the narrow community that is most affected by the TLD. *Id.* See ICANN, *Top Level Domains*, *supra* note 6, for a complete listing of gTLDs and their sponsoring organizations.

19. Michael Geist, *ccTLD Governance Project*, at <http://www.cctldinfo.com/home.php> (last visited Dec. 9, 2003).

20. *See Hearing on Internet Domain Names Before the House Comm. on Energy & Commerce, Subcomm. on Telecomm. & the Internet*, 106th Cong. (2000) [hereinafter *Hearing on Internet Domain Names*], 2001 WL 2005249.

21. *See Name.Space v. Network Solutions, Inc.*, 202 F. 3d 573, 577 (2nd Cir. 2002).

22. Geist, *supra* note 19. Ten ccTLDs are governed through government agencies or departments. In these cases, the relationships are formalized between the ccTLD agencies and their respective governments. Nine ccTLDs are governed through private, for-profit organizations; of these, two (the United States and Japan) have established a contractual relationship with their governments. The other three have established informal relationships with their governments. Twenty ccTLDs are governed through non-profit organizations, four of which have formal, contractual relationships with their respective governments and with ICANN. Five others do not have government agreements. Ten others have informal relations with their governments, and at least three are awaiting formalization of this relationship in the near future (Russia, South Africa, and Italy). One ccTLD is managed by an individual. Five ccTLDs are managed by academic institutions, two that have no relationship with their respective governments.

making procedures. Finally, this Part concludes by briefly discussing the federal antitrust law that applies to ICANN's governance.

A. Pre-ICANN Internet Governance

The Internet began as ARPANET, a system sponsored by the U.S. military to improve rapid communication among government entities.²³ Given the limited size of the ARPANET, the U.S. government left its governance mainly in the hands of one individual.²⁴ As ARPANET grew into the Internet, the one-man governance scheme became unwieldy. The U.S. government, in 1993, decided to delegate governance of the Internet and the DNS to a private entity, Network Solutions, Inc. ("NSI").²⁵ NSI acted as both registry and registrar for three of the seven then-existing gTLDs, *.com*, *.net*, and *.org*.²⁶

From 1993 to 1995, NSI used a first-come-first-serve domain name registration policy,²⁷ a policy which led to "cybersquatting": registration of a trademark as a domain name for the purpose of selling the name back to the trademark holder.²⁸

After trademark holders complained about cybersquatting, NSI developed a rudimentary policy to resolve disputes over domain name ownership. Under the policy, NSI allowed trademark holders to present proof of legitimate interest in a particular domain name by showing that they held a trademark in the name.²⁹ Unfortunately, NSI continued to encounter diffi-

23. See *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 849-50 (1997); Development, *The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1660 (1999).

24. Development, *supra* note 23. Dr. Jon Postel was the individual who, along with a group of graduate students at the University of California, was best known for creating ARPANET. He single-handedly ran ARPANET and the Internet, as it later became known, through the Internet Assigned Numbers Authority ("IANA"). *Id.* at 1661.

At the time of Dr. Postel's advancements, the National Science Foundation, affiliated also with the U.S. government, created a second network similar to that of ARPANET. With the help of Dr. Postel, ARPANET and NSF's network eventually communicated with one another. *Id.* Together, they became known as the Internet. *Id.* at 1660.

25. *Id.*; see also Froomkin & Lemley, *supra* note 11, at 9.

26. See generally Froomkin & Lemley, *supra* note 11.

27. Shuli L. Green, *Launching Trademark Law into Cyberspace: Should the Domain Name System be Federalized?*, 49 ADMIN. L. REV. 1031, 1037 (1997).

28. Michael Tanner, *Trademarks, Internet Domain Names, and the NSI: How Do We Fix a System that Is Already Broken?*, 3 J. TECH. L. & POL'Y 2, 40-50 (1998).

29. See Green, *supra* note 27, at 1040. In response, the domain name registrants were also given a similar opportunity whereby they could demonstrate legitimate interest in the same domain name by proof of their own trademark registration. *Id.* If domain name registrants were able to supply this proof, NSI allowed registrants to keep their do-

culties.³⁰ Common law trademark owners felt disadvantaged because they had no formal registration documentation to prove ownership.³¹ Domain name registrants complained that NSI's policy made it too easy for trademark holders to take or suspend a domain name.³² Because of this and other failures, the U.S. government called for changes to the Internet governance structure once again.

B. Internet Corporation of Assigned Names and Numbers

Hoping to alleviate some of the problems encountered under NSI, the U.S. government, in creating ICANN, formed a centralized decision-making body with broad powers to regulate the Internet and its corresponding DNS.³³

Aside from its thorough decision-making process, the introduction of ICANN has also altered the registry-registrar relationship. Prior to ICANN, NSI served three functions: as a registry, as a registrar, and as the governing body for the Internet and DNS. However, ICANN separated these three functions and now acts only as the governing entity overseeing registrars and registries.³⁴ Today, VeriSign, a private corporation whose focus is Internet security, serves as the exclusive registry for the .com,

main names. However, if domain name registrants were unable to supply such proof, NSI placed the particular domain name on a long-term hold until a court resolved the dispute. *Id.*

30. Tanner, *supra* note 28, at 50.

31. Green, *supra* note 27, at 1045.

32. *Id.* Possibly as a result of NSI's dispute resolution policy, the number of new domain name registrations dropped significantly, from 5,000 per week to a mere 1,300 per week. See Ian C. Ballon, *Using Trademarks to Drive Traffic to Websites and Other E-Commerce Law Issues*, 590 PLI/PAT 111, 175 (2002).

33. The U.S. government created ICANN through a series of contracts and Memoranda of Understanding with the Department of Commerce. See Froomkin & Lemley, *supra* note 11, at 14-18; see also ICANN, *Background*, at <http://www.icann.org/general/background.htm> (last visited Nov. 25, 2003) [hereinafter ICANN, *Background*]. Although headquartered in California, ICANN maintains governance over international Internet and DNS issues. ICANN, *Fact-Sheet*, at <http://www.icann.org/general/fact-sheet.htm> (last visited Mar. 14, 2004). Furthermore, despite the U.S. government's obvious relationship with ICANN, the organization holds itself out as a private-sector entity that oversees the technical coordination of the DNS, independent of any national government control. *Id.* ICANN attempts to create a non-governmental policy making body by including representatives from the business, technical, non-commercial, and academic communities. *Id.*

34. See generally Froomkin & Lemley, *supra* note 11. As mentioned in *supra* Part I.C, ICANN only oversees gTLD registries. It does not have authority over ccTLD registries since these are regulated by agencies and governments outside of ICANN.

.net, and .org gTLDs.³⁵ Other registries maintain the remaining gTLDs and ccTLDs located in other nations. In contrast to VeriSign, these registries either control less popular TLDs or TLDs subject to restrictions.³⁶

Because of the current registry-registrar hierarchy, ICANN alone has the power to make policies regulating and allocating infrastructure services to registries and registrars governing gTLDs.³⁷ Indeed, because ICANN alone has the power to create gTLD registries and registrars, it controls all entry into the registry and registrar markets.³⁸

C. Introduction to Antitrust Law

Critics have noted that some of ICANN's policies seemingly hinder competition, especially in providing new registries and new gTLDs in the domain name market. This section briefly introduces the federal antitrust statute under which ICANN has been accused of hindering competition.

Antitrust law's purpose is to protect competition in order to maintain competitive prices and preserve incentives for improvements in goods and services.³⁹ Under section 2 of the Sherman Act,⁴⁰ every person who "shall monopolize, or attempt to monopolize," a relevant market may be punished.⁴¹ The Supreme Court has defined two elements of monopolization: "(1) the possession of monopoly power in the relevant market, and (2) willful acquisition or maintenance of that power."⁴² The first element, monopoly power, is demonstrated when no substitutes are available in the market for a particular product or service.⁴³ The second element, willful acquisition or maintenance, depends on the origin of a monopoly, or the tactics with which it is maintained.⁴⁴ Factors, such as the monopoly's intentional exclusion of competitors, its use of unduly coercive means to re-

35. See Navin Katyal, *The Domain Name Registration .Bizness: Are We Being "Pulled Over" on the Information Super Highway?*, 24 HASTINGS COMM. & ENT. L.J. 241, 255 (2002). VeriSign took over NSI and its responsibilities as registry for the .com, .net, and .org gTLDs in March 2001 when it acquired NSI, and currently operates NSI as its wholly owned subsidiary. *Id.*

36. See *supra* Part I.C.

37. Tamar Frankel, *The Managing Lawmaker in Cyberspace: A Power Model*, 27 BROOK. J. INT'L L. 857, 873 (2002).

38. *Id.*

39. See, e.g., U.S. Dep't of Justice, *Antitrust Enforcement and the Consumer*, at http://www.usdoj.gov/atr/public/div_stats/9142.htm (last visited Jan. 29, 2004).

40. 15 U.S.C. § 2 (2000).

41. *Id.*

42. *United States v. Grinnell*, 384 U.S. 563, 570-71 (1966).

43. See *United States v. E.I. du Pont De Nemours & Co.*, 351 U.S. 377, 394 (1956).

44. *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 429 (2d Cir. 1945) [hereinafter *Alcoa*].

duce competition, and its course of unnatural growth, play crucial roles in demonstrating the requisite intent.⁴⁵

Section 2 of the Sherman Act does not seek to punish all monopolies and monopolists. The active verb form of "monopolize" is used rather than its noun or adjective form.⁴⁶ From this, the Supreme Court has inferred that the Act does not hold liable those who find themselves in possession of a monopoly if they did not intend either to put an end to existing competition or to prevent competition from arising.⁴⁷ Firms that become monopolists by "force of accident" have no liability under the Act.⁴⁸ Similarly, the Act does not forbid monopolies established through natural growth of a company, or by the mere fact that the company is the "single producer" of a good or service in the market.⁴⁹ Accordingly, a monopolist may escape liability if it can show that it attained monopoly power through "superior skill or products, natural advantages including accessibility to raw materials and markets," economies of scale, or the like.⁵⁰

Aside from monopolization, section 2 also prohibits attempted monopolization of a relevant market.⁵¹ According to the Supreme Court, to demonstrate attempted monopolization, the plaintiff must prove "(1) that the defendant has engaged in predatory or anticompetitive conduct with (2) a specific intent to monopolize, and (3) a dangerous probability of achieving monopoly power."⁵² Dangerous probability requires the proof of

45. *See generally id.* In *Alcoa*, the Second Circuit held that Alcoa had monopolized the aluminum ingot market and violated section 2 of the Sherman Act through its misuse of aluminum production patents, its contracts with power companies (whereby Alcoa disallowed others from selling power to all competing aluminum manufactures), and its collusion with foreign manufactures limiting or eliminating all aluminum imports into the United States. *See generally id.*

46. *Id.* at 429.

47. *Id.*

48. *Id.* at 430.

49. *Id.*

50. *United States v. United Shoe Mach. Corp.*, 110 F. Supp. 295, 342 (D. Mass. 1953), *aff'd*, 347 U.S. 521 (1954) (per curiam). In *United Shoe*, the Court held that the monopolist could not place all of its monopoly power on one or more of the above excuses. *Id.* In fact, the Court found that United Shoe's leasing system, whereby the company leased its superior shoe making machines under certain restrictions, which forced their users to forgo all deals with other shoe machine providers, constituted willful acquisition and maintenance of market power. *Id.* at 340-43. Hence, United Shoe was found liable under section 2.

51. 15 U.S.C. § 2 (2000).

52. *Spectrum Sports v. McQuillan*, 506 U.S. 447, 456 (1993).

“a relevant market, and the defendant’s ability to lessen or destroy competition in that market.”⁵³

Monopoly power has been viewed as a power that “deadens initiative, discourages thrift, and depresses energy.”⁵⁴ In contrast, competition and rivalry are deemed stimulants to industrial progress, and that the “spur of constant stress is necessary to counteract an inevitable disposition to let well enough alone.”⁵⁵ Due to the notion that competition creates savings for consumers, the Sherman Act’s application has been urged by some to extend to ICANN and its policies.⁵⁶

III. ICANN AND ANTITRUST: CURRENT AND FUTURE CHALLENGES

Recently, some commentators have asserted that the structure and operation of ICANN raises antitrust concerns.⁵⁷ Within this Part, section A explores a preliminary question: whether ICANN and its affiliates could be subject to antitrust liability, or whether they are immune from such liability due to their relations with the U.S. government. Section B considers the argument that ICANN may be illegally monopolizing the TLD market. Section C examines a similar contention that ICANN’s policies prohibiting registries from engaging in business relationships with alternative domain name and TLD providers also point toward the organization’s monopolization of the TLD market. Finally, section D discusses VeriSign’s newly proposed wait-listing service and its possible effect on registrars that already provide such a service. The section will explore the merits and criticisms of the proposed wait-listing service, and consider how VeriSign may fall under the attempted monopolization doctrine of section 2 of the Sherman Act.

A. Adjudication of Antitrust Claims Against ICANN and VeriSign

A threshold consideration is whether ICANN and VeriSign are immune to antitrust liability. This section considers the possibility that ICANN and VeriSign may avoid antitrust liability by examining prior antitrust suits brought against ICANN’s predecessor, NSI. It also examines ICANN and VeriSign’s current relationships with the U.S. government and how those relationships affect their liability.

53. *Id.*

54. *Alcoa*, 148 F.2d at 427.

55. *Id.*

56. *See generally* Froomkin & Lemley, *supra* note 11 (arguing throughout the article that ICANN’s current practices require antitrust scrutiny).

57. *Id.*

Under NSI's regime in the 1990s, several trademark holders brought antitrust actions against NSI.⁵⁸ In all cases, the district courts dismissed the claims under the federal instrumentality immunity doctrine, which grants antitrust immunity to contractual parties working for the U.S. government.⁵⁹ On appeal, however, the circuit courts were less lenient. They denied federal instrumentality immunity but nevertheless dismissed the antitrust actions on equity grounds. Specifically, the courts held that a private entity acting pursuant to a government contract should not be punished for carrying out duties as outlined in its contract.⁶⁰

A similar argument could be made in ICANN's case. Because the U.S. government initiated ICANN through a series of understandings and contracts, ICANN acts as a private contractor carrying out the duties given to it by the government. Hence, ICANN could avoid antitrust claims as NSI once did.

This argument, however, is not likely to succeed. Despite the memoranda of understanding and contracts prepared by the U.S. Department of Commerce,⁶¹ the U.S. government created ICANN as an independent, nonprofit organization.⁶² ICANN has also always publicized itself as an independent, non-government entity not bound to the specific needs of the United States but the entire globe.⁶³ Hence, a court would unlikely find ICANN to be a private contractor working solely for the U.S. government.⁶⁴ Instead, a court would more likely find ICANN to be a private entity subject to antitrust scrutiny.⁶⁵

Similarly, VeriSign is also an entirely independent and private entity, even more so than ICANN. Having no relationship to the U.S. government directly or indirectly, VeriSign cannot depend on prior decisions to shield itself from antitrust claims and could be vulnerable to antitrust liability.

B. Monopolization of Top Level Domains

The TLD market, specifically the gTLD market as regulated by ICANN, constitutes a relevant market within the more general domain

58. These lawsuits included *Name.Space v. Network Solutions, Inc.*, 202 F.3d 573, 577 (2d Cir. 2002); *Thomas v. Network Solutions, Inc.*, 176 F.3d 500 (D.C. Cir. 1999); and *Watts v. Network Solutions, Inc.*, No. IP 98-1529-C, 1999 U.S. Dist. LEXIS 20605 (S.D. Ind. May 7, 1999). See also Froomkin & Lemley, *supra* note 11, at 33.

59. Froomkin & Lemley, *supra* note 11, at 33.

60. *Id.* at 34.

61. *Id.* at 24.

62. ICANN, *Background*, *supra* note 33.

63. *Id.*

64. See Froomkin & Lemley, *supra* note 11, at 41.

65. See *id.*

name market. Since domain names are issued through TLDs, consumers may or may not be constrained in their domain name choices depending on the availability of TLDs. Similarly, because registries maintain TLDs, the TLD market is coextensive with the registry market. When there are few registries available to control TLDs, consumers have fewer choices for domain names, and less opportunity to obtain a desired name. As Part II.B noted, ICANN, as the sole controller of entry into and exit out of the registry business, also controls the number of TLDs.

Critics assert that ICANN's slowness in developing new gTLDs and its rigid standards for new applicant registries prevent competition within the registry/TLD market.⁶⁶ Currently, ICANN requires interested registries to pay a \$50,000 nonrefundable application fee.⁶⁷ It also requires applicant registries to have substantial financial backing and well-thought-out plans for undertaking the responsibilities required for maintaining new gTLDs.⁶⁸

Critics allege that these policies hinder competition among registries and ultimately prevent consumer choice. Because registries must engage in a long process to find adequate funding and create a thorough plan, few new registries have emerged. This causes consumers to register domain names under existing registries, few of which are open to the general public.⁶⁹ As a result, many consumers are funneled to the VeriSign registry which controls the most popular and least restrictive gTLDs: *.com*, *.net*, and *.org*. However, fewer and fewer domain names remain available in these popular gTLDs for the vast number of individuals and businesses still interested in registering domain names.

66. *See id.* at 24.

67. *Id.*

68. *See id.* at 52.

69. *See supra* Part I.C. Currently, many registrants, businesses and individuals alike, find themselves registering through VeriSign's controlled gTLDs (*.com*, *.net*, and *.org*). See ICANN, gTLD Registry Best Practices, at <http://www.icann.org/tlds/gtld-registry-best-practices-30sep00.htm> (last visited Mar. 8, 2004) (acknowledging the enormous popularity of VeriSign's *.com*, *.net*, and *.org* gTLDs, and the need to increase VeriSign's capacity to deal with an increasing volume of domain name registrations). Presently, VeriSign has found a need to increase its daily volume by 500% and reduce its down time by over 75%. *Id.* This increase in volume in the VeriSign registry has prompted ICANN to issue reports such as the "gTLD Registry Best Practices" article in hopes of extending an invitation to potential applicant registries to join the registry business and satisfy customer's demand for domain names. *See id.* The article also sets out ICANN's standards for such applicant registries. *See id.*

Currently, many registrants, businesses and individuals alike, find themselves registering only through VeriSign's controlled gTLDs (*.com*, *.net*, and *.org*) because these gTLDs are not restricted to any specific organizations or for any specific purposes.

Critics argue that ICANN's current conduct conforms to that of an organization in the process of monopolizing a market, particularly the TLD/registry market.⁷⁰ Because the United States government, in institutionalizing ICANN, instilled in it the power to regulate the registry business,⁷¹ ICANN possesses sole power in determining entry and exit of such businesses in the TLD/registry market. Therefore, the first element of a section 2 violation could conceivably be established.

However, demonstrating that ICANN also meets the second element of section 2's monopolization test presents a greater challenge. Critics allege that ICANN's slowness in initiating new gTLDs and new registries is indicative of its willfulness in preventing free market competition within this market.⁷² On the other hand, ICANN asserts that its seemingly monopolistic actions are justified by the necessity (1) for Internet stability and (2) to protect the interest of trademark holders. First, in support of its Internet stability argument, ICANN suggests that its strict policies for funding and organization ensure that a newly elected registry would be able to properly maintain a new gTLD. This provides a stable gTLD that allows trademark holders, firms, and individuals to invest in domain names with confidence.⁷³

Second, ICANN points out that many trademark holders may appreciate its strict policies.⁷⁴ Whenever ICANN introduces a new, unrestricted registry and new gTLD, trademark holders must race to register all of their trademarks within this gTLD before cybersquatters do.⁷⁵ This presents an enormous burden and is very costly for trademark holders with many trademarks such as large, multi-international companies. Therefore, ICANN's apparent willful acquisition of power within the TLD/registry market is in fact the organization's method of achieving better products and service for the Internet consumer. It is likely that ICANN's strict policies help consumers more than they harm them, so an antitrust plaintiff is unlikely to be able to prove that ICANN abuses its monopoly power.

70. See generally Froomkin & Lemley, *supra* note 11, at 56.

71. See *supra* Part I.C.

72. See generally Froomkin & Lemley, *supra* note 11.

73. See Edward Brunet, *Defending Commerce's Contract Delegation of Power to ICANN*, 6 J. SMALL & EMERGING BUS. L. 1, 6 (2002).

74. See Froomkin & Lemley, *supra* note 11, at 24; see also *Hearing on Internet Domain Names*, *supra* note 20.

75. See generally Froomkin & Lemley, *supra* note 11.

C. Extending Monopolization of TLD market by Eliminating Alternative Domain Name Systems

ICANN's DNS is not the only possible domain name system available on the Internet. Alternative domain name systems, although rather uncommon, have created alternative TLDs outside of ICANN's grasp. In order to do this, alternative DNS providers, while utilizing ICANN-controlled legacy root files for common gTLDs such as *.com*, *.net*, and *.org*,⁷⁶ create different TLDs within these legacy roots by using supersets of these roots.⁷⁷ Suppose that a user who is served by an alternative DNS provider types "law.web" as an address query into the Internet. The ICANN legacy root files will not recognize *.web* as a legitimate gTLD since it has never been created. However, alternative DNS providers would re-route this query to their privately operated registries that maintain the *.web* gTLD, if *.web* were one of their created gTLDs.⁷⁸ In this way, alternative DNS providers have created a service network outside of ICANN-controlled gTLDs.

Currently, ICANN operates under a policy which prohibits all ICANN affiliated registries from servicing alternative DNS providers.⁷⁹ Without the support of able registries, critics are concerned that alternative providers face difficulty in managing their TLDs and attracting consumers.⁸⁰ Consequently, this has prompted criticism that ICANN is again trying to prevent competitors from emerging and potentially threatening ICANN-regulated TLDs. This suggests that ICANN is again monopolizing the TLD market.⁸¹

Upon examination, one could argue that ICANN's conduct meets both elements of the monopolization test under section 2 of the Sherman Act. First, ICANN appears to possess monopoly power in the TLD market as suggested by section A above. Second, ICANN may meet the intent re-

76. Each TLD is controlled by a legacy root file which maintains all of the second level domains and address queries within the particular TLD. See Froomkin & Lemley, *supra* note 11, at 7.

77. *Id.* at 20-21. To do this, alternative DNS service providers use supersets of ICANN-controlled legacy roots. Rather than getting domain names from a member registry of the legacy root hierarchy controlled by ICANN, such as from the *.com* gTLD, users of alternative DNS roots instead get DNS service from a provider who obtains its data from a different root file. *Id.* at 20.

78. *Id.* at 21.

79. *Id.* at 52-53.

80. *Id.*

81. *See id.*

quirement through its prohibitive policies toward registries in relation to alternative DNS providers.⁸²

Nevertheless, whether ICANN is truly monopolizing the TLD market still remains to be seen. Evidence countering the above criticisms suggests that despite ICANN's restrictive policy, alternative DNS providers do exist and do compete against ICANN's DNS. For example, alternative DNS provider New.net has created a separate system where New.net bases its Internet domain names on twenty new Top Level Domain extensions such as ".xxx" and ".sport."⁸³ To better compete against ICANN, it has encouraged web users to download plug-ins that allow browsers to recognize alternative domain name systems.⁸⁴ New.net, along with other alternative DNS providers, have negotiated with several Internet Service Providers (ISPs) to include service to alternative DNS providers as part of the ISPs' plans.⁸⁵ From this evidence, it is unclear whether ICANN truly satisfies section 2's monopolization test since competitors have surfaced in the face of ICANN's no-contact policies. Specifically, it is unclear whether ICANN truly possesses monopoly power in the TLD market in relation to these alternative DNS providers.

D. Attempted Monopolization of Wait-Listing Services

The final set of criticisms against ICANN involve VeriSign's proposal to create its own Wait-Listing Service ("WLS") for the .com, .net, and .org gTLDs. A wait-listing service allows individuals to automatically acquire or re-acquire a domain name once the domain name's registration period ends. Currently, registrants obtain domain names for one to two years. When this period expires, registrants must renew the names, or else they will become available for public registration. Every year, many businesses

82. In *Alcoa*, the Second Circuit held that Alcoa's covenants with power plants to prohibit their dealing with competing aluminum producers was indicative of Alcoa's willful intent to monopolize the aluminum ingot market. *See generally Alcoa*, 148 F.2d 416 (2nd Cir. 1945). Similarly, an argument could be made here that ICANN's covenants with registries prohibiting them from engaging in relationships with alternative DNS providers also is indicative of ICANN's will to monopolize the TLD market.

83. Froomkin & Lemley, *supra* note 11, at 21; Katyal, *supra* note 35, at 267.

84. *See generally* Froomkin & Lemley, *supra* note 11. For instance, New.net's plug-in has the computer add "new.net" to every query entered by the web user such that all queries will be correctly directed to New.net's system.

85. *Id.* at 21-22. Internet Service Providers are those private entities that offer Internet services and allow businesses and Internet users to log onto the World Wide Web through their computers. For the most part, their services route all Internet queries to ICANN's DNS.

and individuals who fail to renew their registrations lose them to others who seize the opportunity to register these names as their own.⁸⁶

Today, nearly sixty registrars offer wait-listing services for individuals interested in acquiring soon-to-expire domain names.⁸⁷ For example, SnapNames, a United States-based registrar, looks for soon-to-expire domain names available through the VeriSign registry. SnapNames lists these names on its own website, and interested registrants can request that SnapNames register the name for them when it becomes available.⁸⁸ When SnapNames successfully registers a domain name for a customer, SnapNames becomes the registrar for that name.⁸⁹

Other registrars offer slightly different versions of wait-listing services. Dotster, another United States-based registrar, allows interested registrants to bid on soon-to-expire domain names.⁹⁰ Dotster then attempts to snatch each domain name as it becomes available from the VeriSign registry and then resell the name to the highest bidder.⁹¹

Wait-listing services constitute their own relevant market within the domain name market because they are a unique set of services serving only those interested consumers who want to acquire someone else's expired domain name.⁹² Wait-listing services require technological sophistication different than that needed in registering a domain name. For instance, the success of snatching a soon-to-expire domain name depends on the technological capabilities of a registrar.⁹³

Today, the sixty-some registrars offering wait-listing services are competitive in three ways. First, pricing for wait-listing services is reduced due to fierce competition for customers.⁹⁴ Second, competition in the wait-

86. Margaret Kane, *VeriSign Preps Wait List for Coveted .coms*, CNETNEWS.COM, Jan. 4, 1999, at <http://news.com.com/2100-1023-801085.html?legacy=cnet>.

87. Rita Mezzanotte, *Pool.com Launches ICANN Lawsuit Against WLS*, CIRCLEID (July 10, 2003), at http://www.circleId.com/article/160_0_1_0_C; *Wait List Gives Cause for Concern*, DEMYS NEWS SERV. (Feb. 5, 2002), at http://www.demys.net/news/2002/02/02_Feb_05_wait_list.htm.

88. See Mezzanotte, *supra* note 87; see also Froomkin & Lemley, *supra* note 11, at 65.

89. See Mezzanotte, *supra* note 87.

90. *In the Land of the Free*, DEMYS NEWS SERV. (June 25, 2003), at http://www.demys.net/news/2003/06/25_free.htm.

91. See *id.*

92. See Froomkin & Lemley, *supra* note 11, at 65.

93. *In the Land of the Free*, *supra* note 90.

94. For example, Pool.com, a Canada-based registrar, in order to attract customers, has instituted a policy that does not require up-front charges for backorders. Mezzanotte, *supra* note 87. It will only charge a fee once Pool.com successfully acquires the expired domain name and registers it in the customer's name. *Id.*

listing service market enhances innovation in acquiring domain names. For registrars to improve their wait-listing services and to attract more customers, they feel the incentive to constantly upgrade their technology to be the first to acquire a domain name.⁹⁵ Finally, the competition enhances consumer choice. A consumer dissatisfied with one service can try another. With more than one wait-listing service, consumers are more likely to find a provider whose service they enjoy.

Critics allege that VeriSign's proposal will undermine competition and remove these consumer advantages in the wait-listing service market.⁹⁶ Since VeriSign is the registry for the most popular gTLDs, it would be able to re-register a domain name in these gTLDs before any of the competing registrars. This would obliterate any competition in the wait-listing service market.

The above criticisms suggest that VeriSign may be liable for attempted monopolization.⁹⁷ Under the first element of attempted monopolization, VeriSign seemingly engages in anticompetitive conduct by proposing a plan which could effectively eliminate all other WLS providers. Under the second element, VeriSign's proposal, on its surface, has the intent to monopolize the WLS market since its proposal would grant all WLS ability solely to VeriSign. Finally, under the third element, if the proposal were implemented, VeriSign might not only have a dangerous probability of achieving monopoly power, it might have almost the entire wait-listing service market since *.com*, *.net*, and *.org* are the most popular and most heavily used TLDs.⁹⁸ Hence, VeriSign could conceivably achieve monopoly unless it exercises some form of restraint.

VeriSign rationalizes its proposal with an argument similar to ICANN's: its proposal would instill stability and predictability in the domain name system by ensuring that at least one customer would obtain the soon-to-expire domain name.⁹⁹ However, VeriSign's contention has less merit than those asserted by ICANN. Unlike ICANN, whose prerogatives of providing financially sound registries and gradually increasing the

95. See *In the Land of the Free*, *supra* note 90.

96. Some registrars, including Dotster and Pool.com, have initiated lawsuits against VeriSign for antitrust violations. See *ICANN: VeriSign's 'Wait List' Service is Illegal, Complaint Alleges*, 21 ANDREWS COMPUTER & ONLINE INDUS. LITIG. REP. 12 (2003); see also *In the Land of the Free*, *supra* note 90.

97. See *supra* Part II.C.

98. Compare these three elements to the three elements required under the attempted monopolization test as specified in *Spectrum Sports v. McQuillan*, 506 U.S. 447, 456 (1993).

99. Froomkin & Lemley, *supra* note 11, at 65.

number of TLDs have at least some substantial merit against allegations of monopolization, VeriSign's proposal lacks merit against allegations of attempted monopolization. In fact, its proposal, if enacted, eliminates an enormous number of competitors and appears to lack a purpose other than that of attempted monopolization of the WLS market. Hence, it is much more likely that VeriSign's proposal would face a considerable challenge in defeating an attempted monopolization claim.

IV. CONCLUSION

Based on the discussion in this Note, ICANN and VeriSign may be subject to antitrust liability because they are independent, private organizations. However, the current claims against ICANN may have little merit. ICANN's policies and actions may be necessary to maintain a stable Internet and may not hinder competition to such a degree as to create a monopoly in the domain name market. Therefore, it is unlikely that ICANN would presently be subject to antitrust litigation. Criticisms against VeriSign, on the other hand, have more validity since its proposal to do away with competing wait-listing services appear to be an attempt at monopolization. Hence, it is more likely for VeriSign to face antitrust litigation. Nevertheless, all claims against ICANN and VeriSign would depend on the decisions made by our courts, who could become the ultimate deciders in whether Internet governance needs to have yet another round of changes.

BERKELEY TECHNOLOGY LAW JOURNAL