ICANN AND ANTITRUST[†]

*A. Michael Froomkin**
*Mark A. Lemley***

The Internet's smooth functioning depends on the domain name system (DNS), which allows users to enter an address into their browser and be directed to the appropriate web site or e-mail recipient. In 1998, the Department of Commerce (DoC) delegated effective control over the DNS to a private, not-for-profit corporation, the Internet Corporation for Assigned Names and Numbers (ICANN). Various aspects of ICANN have been heavily criticized by commentators. In this article, Professors Froomkin and Lemley address the previously neglected issue of whether ICANN and its policies violate U.S. antitrust law.

Professors Froomkin and Lemley begin by analyzing whether ICANN would be immune from antitrust scrutiny under the state action doctrine. This would be unlikely, they conclude, because there has been no clear articulation of policy nor active supervision by the government. The authors then consider the merits of four potential antitrust challenges: that the DNS and top level domains such as .com are essential facilities to which ICANN must give open access; that ICANN's refusal to accredit registrars affiliated with alternative roots is an act of monopolization; that ICANN's requirement that registrars adhere to a uniform dispute resolution policy for trademark disputes is an illegal cartel; and that VeriSign's "Waiting List Service," approved by ICANN, is an exclusive dealing arrangement with anticompetitive consequences. Additionally, since ICANN is not a government actor, the authors warn that those who lobby ICANN could also be liable for any antitrust law violations.

Professors Froomkin and Lemley conclude that delegating extensive policy-making authority to ICANN without providing any

* *Professor of Law, University of Miami School of Law. I should disclose that I was involved in some of the events discussed in this article.*

** *Professor of Law, Boalt Hall, University of California at Berkeley; of counsel, Keker & Van Nest LLP.*

We would like to thank Caroline Bradley, Roger Fearing, Rose Hagan, Cedric Manara, David McGowan, Gary Minda, Michael Palage, Tony Rutkowski, Polk Wagner, Phil Weiser and participants at the Telecommunications Policy Research Conference for comments on an earlier draft and Collen Chien for research assistance.

means of accountability causes unanticipated antitrust problems. If ICANN is subject to antitrust law, the authors assert, it will have to reevaluate its policies of excluding alternate roots and requiring registrars to adopt its uniform dispute resolution policy. Professors Froomkin and Lemley ultimately conclude that the U.S. government should either assume a more active role in setting domain name policy or, in the alternative, let the market operate unfettered.

The Internet domain name system (DNS) is an addressing system that greatly facilitates Internet communication. Users who type a domain name into their computer are able to send a message to, or view web pages created by, the party who "owns" that domain name only because there is a database somewhere that links domain names to the unique identifying numbers that the Internet needs to route data properly. In the late 1990s, the U.S. government ceded de facto technical and policy control over the DNS to a private non-profit company. That company, the Internet Corporation for Assigned Names and Numbers (ICANN), acts as the de facto regulator for DNS policy. It makes the rules about what will go in the master addressing database that almost everyone on the Internet ultimately relies on for every Internet communication. In addition to technical policy coordination, ICANN also engages in policies that strongly resemble traditional regulation of market structure. It decides what top-level-domains (TLDs)[1] will be made available to users, what policies new TLDs will have to follow, and who will be permitted to offer domain names in those TLDs for sale to the public.[2] And it makes those decisions at least in part based on the potential seller's willingness to offer a package of services that includes mandatory trademark arbitration.

ICANN's curious status as a quasi-nongovernmental organization with strong ties to the government has occasioned a good deal of comment,[3] much of it negative.[4] Some of that comment has focused on

1. Top-level domains include international generic domains (gTLDs) such as .com and .net and country-code domains (ccTLDs) such as .uk and .ca.

2. Domain name registries maintain the top-level domains that are used for addressing the Internet. Registrars are the companies that actually register domain names in the registries, usually charging registrants for the service.

3. For a detailed discussion of those ties, and the history of ICANN more generally, see A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17 (2000) [hereinafter Froomkin, *Wrong Turn*]; Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2000) [hereinafter Weinberg, *Problem of Legitimacy*]; Jonathan Weinberg, ICANN, "Internet Stability," and New Top Level Domains (Jan. 30, 2002) (unpublished draft), *available at* http://www.law.wayne.edu/weinberg/icannetc.pdf [hereinafter Weinberg, ICANN and New TLDs] (on file with the University of Illinois Law Review); *see also* Laurence Helfer & Graeme Dinwoodie, *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*, 43 WM. & MARY L. REV. 141 (2001); Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89 (2001); Jessica Litman, *The DNS Wars: Trademarks and the Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149 (2000); Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163 (1999).

ICANN's rather fitful starts towards open and participatory governance of the DNS.[5] Others have questioned the legitimacy of handing important policy questions over to a private—or at least mostly private—entity.[6] In this article, we focus on a hitherto-neglected implication of ICANN's private status: its potential liability under the U.S. antitrust laws, and the liability of those who transact with it.

ICANN finds itself on the horns of a dilemma. It has some of the indicia of a government corporation exercising authority granted to it by the Department of Commerce (DoC).[7] If ICANN is therefore a state entity, it is subject to both constitutional constraints on its regulatory authority, notably the requirement of due process,[8] and to statutory limits on the authority that can be delegated to it by the DoC, notably the burdens of the Administrative Procedures Act.[9] Neither ICANN's actions nor those of the DoC in regards to DNS policy to date satisfy those procedural constraints. Both ICANN and the U.S. government argue that ICANN is not subject to those rules because it is a private industry self-regulatory body.[10] Although one of us has argued that ICANN is best understood to be a state actor for constitutional law purposes,[11] the contrary argument that ICANN is private is not without merit. If ICANN is private, however, it follows that both ICANN and private actors who have relationships with it are subject to U.S. (and probably non-U.S.) antitrust law.

Previous legal efforts to subject the Internet Assigned Numbers Authority (IANA) and Network Solutions, Inc. (NSI)—ICANN's predecessors in running the DNS—to U.S. antitrust liability have uniformly failed.

4. Some of the harshest criticism has come from within. On February 24, 2002, ICANN President and CEO Stuart Lynn issued a roadmap for reform of ICANN. The document combined stinging self-criticism with a plan for a radical restructuring of ICANN. It also proposed increasing ICANN's budget and coercive powers, including a direct take-over of all thirteen of the DNS root servers. *See* M. Stuart Lynn, *President's Report: ICANN—The Case for Reform*, *available at* S://www.icann.org/general/lynn-reform-proposal-24feb02.htm (last modified Feb. 24, 2002) (on file with the University of Illinois Law Review).

5. *See, e.g.*, Weinberg, *Problem of Legitimacy*, *supra* note 3; Jonathan Weinberg, *Geeks and Greeks*, 3 INFO 313 (2001), *available at* http://www.law.wayne.edu/weinberg/p313_s.pdf (on file with the University of Illinois Law Review).

6. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 141–59 (questioning the legality of the government's delegation of policy authority to ICANN); Joseph P. Liu, *Legitimacy and Authority in Internet Coordination: A Domain Name Case Study*, 74 IND. L.J. 587, 604 (1999); Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation*, 71 U. COLO. L. REV. 1263 (2000); Jonathan Zittrain, *ICANN: Between the Public and the Private*, 14 BERKELEY TECH. L.J. 1071 (1999). *But see* Edward Brunet, *Defending Commerce's Contract Delegation of Power to ICANN*, 6 J. SMALL & EMERGING BUS. L. 1 (2002); Joe Sims & Cynthia L. Bauerly, *A Response to Professor Froomkin: Why ICANN Does Not Violate the APA or the Constitution*, 6 J. SMALL & EMERGING BUS. L. 65 (2002).

7. On government corporations, see generally A. Michael Froomkin, *Reinventing the Government Corporation*, 1995 U. ILL. L. REV. 543 [hereinafter Froomkin, *Reinventing*].

8. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 94–96 (summarizing case law).

9. *See* 5 U.S.C. §§ 551–559 (2000).

10. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 94–96.

11. *See id.* at 117–18; *cf.* Josh A. Goldfoot, *Antitrust Implications of Internet Administration*, 84 VA. L. REV. 909, 924–27 (1998) (concluding NSI was not a state actor for constitutional purposes).

This is at least in part because the courts concluded that the pre-ICANN DNS was run by state actors or those (such as NSI) acting at their behest, and was therefore immune from antitrust scrutiny.[12] ICANN argues, however, that it is not as closely tied to the government as NSI was in the days before ICANN was created.[13] If this argument is correct, it seems likely that ICANN will not benefit from the same immunity. Rather, it will have to defend its actions on their competitive merits. In this article we consider the antitrust implications of ICANN's actions, both for it and for those who interact with it.

Some of ICANN's regulatory actions clearly raise competitive concerns. For example, in the recent round of applications for new TLDs, ICANN made it a prime requirement that applicants demonstrate that their proposals would not enable competitive (alternate) roots—potential competitors to ICANN. Similarly, ICANN prevents certain types of nonprice competition among registrars by requiring that they adhere to an ICANN Uniform Dispute Resolution Policy (UDRP) that was, in substantial part, drafted by a consortium of existing registrars.[14] ICANN's rules—coupled with its de facto control over the DNS—may have the effect of restraining competition, though they may also be justified on other grounds.

Furthermore, the process by which those rules were adopted might be characterized as anticompetitive collusion by existing registrars. Those registrars will not likely be subject to the *Noerr-Pennington* lobbying exemption that would shield them from antitrust immunity were ICANN a public body.[15] ICANN sets these and other policies within a structure that gives the 'regulated' a strong voice in the policies applied to them: half of the ICANN Board seats are allocated by representatives of industries and groups potentially affected by ICANN's actions.[16]

12. *See infra* notes 159–73 and accompanying text (discussing these cases).

13. *See infra* notes 209–12 and accompanying text.

14. *See infra* notes 124–39 and accompanying text.

15. Antitrust immunity grew out of *Eastern Railroad Presidents Conference v. Noerr Motor Freight, Inc.*, 365 U.S. 127 (1961) and *United Mine Workers v. Pennington*, 381 U.S. 657 (1965). For background on the source of the doctrine, see David McGowan & Mark A. Lemley, *Antitrust Immunity: State Action and Federalism, Petitioning and the First Amendment*, 17 HARV. J.L. & PUB. POL'Y 293 (1994). We discuss the nature of *Noerr-Pennington* immunity in more detail in *infra* notes 349–52 and accompanying text.

16. ICANN is currently considering a proposal to reduce the Board to fifteen persons, eight of whom would be selected by a committee appointed by the Board itself, two representing ccTLDs, two representing registrars, two representing the bodies that assign IP numbers, and two representing an amalgam of registries and ISPs providing gTLD-related services and (some) users of gTLDs, plus the President *ex officio*. *See* Comm. on ICANN Evolution & Reform, *ICANN: A Blueprint from Reform*, *available at* http://www.icann.org/committees/evol-reform/blueprint-20jun02.htm (June 20, 2002) (on file with the University of Illinois Law Review). For a stinging assessment of this process, see Posting of Danny Younger, DannyYounger@cs.com, to reform-comments@icann.org (Sept. 10, 2002), *available at* http://forum.icann.org/reform-comments/implementation/msg00015.html (on file with the University of Illinois Law Review) (arguing that the membership of proposed NomCom is stacked to favor the same interests that currently control the ICANN Board).

Whether ICANN has in fact violated the antitrust laws depends on whether it is an antitrust state actor (even if it is not, by hypothesis, a state actor for purposes of constitutional law), whether the DNS is an "essential facility" under the antitrust laws, on the extent of ICANN's "government contractor" immunity under an unusual zero-dollar procurement contract, and on whether it can shelter under precedents that protect standard-setting bodies. Particular attention under antitrust law will be paid to the extent to which the government has both clearly articulated a policy direction for ICANN and actively supervised ICANN's performance of its duties. While Congress is presently investigating ICANN, a plausible argument can be made that the government has neither clearly articulated support for nor actively supervised ICANN's anticompetitive actions. If so, it will be treated just as any other private market participant would be treated. The exposure of those outside of ICANN who take part in ICANN's constituencies, and who lobby ICANN in a collective manner to impose rules on them and their competitors, depends in part on ICANN's status as a quasi-state actor. It also depends on the nature of their conduct, how closely they coordinate behavior, and the effect on competition.

If (as seems likely) ICANN and those who petition it are subject to antitrust law, everyone involved in the process needs to review their conduct with an eye towards legal liability. ICANN should act very differently with respect to both the UDRP and its treatment of potential competitors if it is to avoid restraining trade. Whether ICANN's UDRP and competitive root policies are desirable is another matter, one on which the authors do not necessarily agree. But if ICANN's policies are in fact desirable, then it seems clear that the government must take a more active role both in setting those policies and in supervising their implementation, either by exercising control over ICANN or by replacing it with a true governmental decision maker. Although ICANN is currently engaged in a round of internal structural reform,[17] it seems unlikely that the degree of government involvement in ICANN will grow substantially. So long as ICANN remains plausibly private, it seems likely that these recommendations will continue to apply with equal force to a restructured ICANN.

In part I, we briefly review ICANN's history and its relationship to the U.S. government. Part II discusses the antitrust state action doctrine, how that doctrine has been applied in the past to the DNS, and how it would likely apply to ICANN. In part III, we focus on several ICANN policies that are potentially anticompetitive, including its restriction on the deployment of new TLDs and its decision to require a uniform arbitration procedure for resolving trademark disputes. Finally, part IV con-

17. *See* Lynn, *supra* note 4.

siders the liability of other private parties who petition ICANN to set its policies.[18]

I. ICANN IN A NUTSHELL

ICANN is a complicated answer to two problems, one technical and one political. The technical problem results from the architecture of the DNS on which the smooth functioning of the Internet relies. The Internet is a giant network of machines that use common protocols to communicate with one another. Every resource on the network has a unique address, called an Internet Protocol (IP) number.[19] Because IP numbers are hard for people to remember, Internet standards provide for the creation of mnemonic names for resources. The DNS is the name given to the complex system for registering those mnemonics—domain names—and maintaining the vast distributed directories that permit every browser pointed at a Uniform Resource Locator (URL) to look up the correct IP number and deliver an Internet communication, and every e-mail to reach its destination. The act of looking up a domain name and retrieving the associated IP numbers is called *name resolution*.

The original design of the DNS assumed that there would be one hierarchically organized set of domain names, and that every domain name in it would be unique. Unique domain names ensure that every Internet user who types a particular URL will find that it resolves to the same IP number associated with that URL, and thus allows a connection to the same resource. The failure to ensure uniqueness—to allow a condition where different users typing the same thing get routed to different IP numbers—has been called a "name collision," or more pejoratively,

18. Although there are parallels between ICANN and other quasi-public authorities that regulate naming conventions, we do not discuss them in this article. Antitrust analysis of this type is heavily dependent on facts which may vary substantially from case to case. The analysis of immunity, for example, depends on the precise nature of the naming entity's relationship with government(s), and just how "essential" the resource is to competitors. There are parallels between ICANN's control over top-level domain names and the (ICANN-endorsed) monopoly of Regional Internet Registries (RIRs) over IP numbers, but there are also differences. Similarly, the proposal for a centralized international ENUM standard that would use the DNS system to store and retrieve telephone-related data may raise similar questions. We leave these for another day.

19. People use the IP numbers they have been assigned in different ways. Some IP numbers are "static," i.e., assigned to the same resource for long periods of time; others (most typically IP numbers used by Internet service providers) are "dynamic," i.e., shared out and then withdrawn on an as-needed basis, i.e., to a user for the length of a dial-up connection via modem, or perhaps on a daily basis for DHCP-based DSL or cable connections. A typical DNS record for a second-level domain name contains several resource records. There will usually be the main "resource record," the "A" record, which lists the default IP number for the domain. There can also be several other specialized resource records in the DNS entry. For example, the entry might typically contain an "MX record" that would be returned for e-mail queries. The MX record is typically a domain name, which itself must then be transformed into an IP number by a second lookup in the domain name system. Many DNS servers are configured to "volunteer" this information to save time.

"instability" of the Internet."[20] To avoid these problems, the DNS relies on a system of layered registrations. In what is sometimes called the "legacy DNS"—the DNS that today almost everyone uses—there is one master file called the "root file" that lists the approved TLDs. Each line in this file contains the name of a TLD and the IP number of a computer that has the authoritative "registry" for that TLD. The root file is copied by the thirteen "root servers," which are the computers that actually resolve any TLD queries that cannot be resolved in hierarchically organized, cached databases closer to the user.

So long as everyone relies on the same family of hierarchically organized databases, whoever controls the root file enjoys the power to determine which TLDs are accessible to the entire Internet, and what registry's database will be considered the authoritative source of information for that TLD. The database of registrations in each TLD is in turn controlled by a single registry.[21] In contrast, today a group of highly competitive "registrars" provide the service of selling actual entries, or registrations, into the registries. To get the right to use a domain name,[22] a registrant in a generic TLD (gTLD) first must find an available name. She then pays a registrar to inscribe her name, contact information, and IP number in the registry. Domain names in .com, .org, and .net and in most of the "country-code" TLDs (ccTLDs) are allocated on a first-come, first-served basis. Names in the newer gTLDs will be allocated in more complex fashions that give priority to trademark holders, and also seek to level the playing field for similarly situated applicants competing for a name during the initial "land rush" period when registrations open.[23]

20. *See, e.g.*, M. Stuart Lynn, ICANN, *ICP-3: A Unique, Authoritative Root for the DNS*, *available at* http://www.icann.org/icp/icp-3.htm (July 9, 2001) (on file with the University of Illinois Law Review) [hereinafter Lynn, *ICP-3*] (stating "alternate roots . . . could cause conflicts and instability").

21. There is no technical reason why one registry cannot control multiple gTLDs—and indeed, VeriSign currently controls three and provides the "back end" service for several others, including .edu, .cc, .tv, and .biz.

22. Whether a registrant acquires a property interest in a domain name, or merely enjoys a service contract is a controversial question. To date the trend seems to be away from a property right, even though the right is something that can be subject to an in rem action. *See, e.g.*, Famology.com, Inc. v. Perot Sys. Corp., 158 F. Supp. 2d 589 (E.D. Va. 2001) (domain name not property subject to a conversion claim); Kremen v. Cohen, 99 F. Supp. 2d 1168, 1173 (N.D. Cal. 2000); Dorer v. Arel, 60 F. Supp. 2d 558, 560–62 (E.D. Va. 1999); Zurakov v. Register.com, Inc., No. 600703/01 (N.Y. Sup. Ct. July 25, 2001), *available at* http://www.courts.state.ny.us/comdiv/law_report_-_October2001.htm (on file with the University of Illinois Law Review); Express One Int'l v. Steinbeck, 53 S.W.3d 895 (Tex. App. 2001).

23. *See* NeuLevel, *.Biz Fact Sheet*, *available at* http://www.neulevel.biz/press/press-kit/fact_sheet.pdf (last visited Oct. 18, 2002) (on file with the University of Illinois Law Review); Afilias Global Registry Services, *The History of .INFO*, *available at* http://www.afilias.info/about_info/info_history (last modified June 21, 2002) (on file with the University of Illinois Law Review).

This process has been marked by substantial controversy. NeuLevel's rollout of the .biz domain used a system by which applicants for popular names could increase their chances of being selected by submitting multiple registrations. A class action claim filed in Los Angeles Superior Court alleged that as each registration request required a nonrefundable fee, the system amounted to an unlicensed and thus illegal lottery. The claim was sufficiently persuasive for Judge Mohr to state that it was

Thus, the legacy DNS system has two chokepoints. Whoever controls the root controls which, and how many, TLDs will be accessible to the vast majority of Internet users. And while there can be many competing registrars, and many TLDs competing with each other, each TLD must have one master registry. A registrar can serve as many different registries as will deal with it. Thus, there is no natural limit on the number of registrars, but for all practical purposes the degree of competition in the upstream registry market is determined by the number of TLDs in the legacy DNS. As for control of the root itself, what competition there is—and it is not much—for the body controlling the legacy root zone is provided by the existence of so-called alternate roots.[24]

The existence of these chokepoints over the legacy root created a political problem. In effect, whoever controlled the root file controlled both whether a given TLD could be part of the Internet and who got the potentially lucrative job of running the TLD's registry. And, by 1997, these were increasingly controversial questions that landed in the lap of the U.S. government, which found itself controlling the root.[25]

From the viewpoint of high-level policy makers, this power was a not-entirely-welcome accident. A series of largely informal arrangements, mostly coordinated by one person, Dr. Jon Postel, and supported by a series of first military, then National Science Foundation contracts,[26]

"more probable than not" that this amounted to an illegal lottery under California law and issue a preliminary injunction barring the registration of contested names. *See* Smiley v. NeuLevel, No. BC 254659 (Cal. Super. Ct. Oct. 11, 2001) (order granting preliminary injunction); Gwendolyn Mariano, *Judge Puts Breaks on .biz Addresses*, CNET (Oct. 12, 2001), *available at* http://news.com.com/2100-1023-274367.html (on file with the University of Illinois Law Review). As some of the plaintiffs were unable to post the security bond required to maintain the injunction, it dissolved, but the case continues. *See* Bret Fausett, *Smiley PI Order Clarified*, ICANN BLOG (Oct. 19, 2001), *available at* http://www.lextext.com/icann/october2001.html (on file with the University of Illinois Law Review).

Meanwhile, the .info "sunrise" period, the advance registration opportunity for trademark owners only, was marred by widespread fraudulent registrations of names based on nonexistent and often obviously bogus trademark registrations. *See* Robert A. Conner, *Study of Over 11,000 .INFO Sunrise Registrations Analyzes Violations of Trademark Submission Rules*, DOME BASE (Aug. 17, 2001), *available at* http://www.DomeBase.com/study.htm (on file with the University of Illinois Law Review). Neither Afilias, the .info registry, nor the registrars, appear to have done any validity checking. *See, e.g.*, Jonathan Weinberg, *One Company Alone Grabbed 1600 .info Domains*, ICANNWATCH (Sept. 6, 2001), *available at* http://www.icannwatch.org/article.php?sid=341 (on file with the University of Illinois Law Review). In addition, the servers for the new registry went down for two days almost immediately after going live. *See* A. Michael Froomkin, *Meltdown: Info Registry Closes for Emergency Maintenance on Day 2*, ICANNWATCH (Oct. 2, 2001), *available at* http://www.icannwatch.org/article.php?sid=396 (on file with the University of Illinois Law Review). Similar problems marred the introduction of later TLDs. *See, e.g.*, Richard Henderson, *Dan Halloran Challenged on Registrars and ICANN's Responsibilities*, ICANNWATCH (May 12, 2002), *available at* http://www.icannwatch.org/article.php?sid=735 (on file with the University of Illinois Law Review).

24. *See infra* notes 95–98 and accompanying text.

25. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 51–62.

26. *See generally* Vint Cerf, *A Brief History of the Internet and Related Networks*, INTERNET SOCIETY, *available at* http://www.isoc.org/internet/history/cerf.shtml (last modified Nov. 18, 2001) (on file with the University of Illinois Law Review) (documenting the creation and growth of the Internet); Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOCIETY, *available at* http://www.isoc.org/internet/history/brief.shtml (last modified Aug. 4, 2000) (on file with the University of Illinois Law Review) (reviewing the origin and fundamental ideas behind the Internet).

had morphed into something unforeseen, important, and increasingly controversial. DNS management had taken on a commercial life of its own due to an explosion of interest in the Internet. Thanks in part to marketing efforts by NSI—which enjoyed a government-granted monopoly on selling domain name registrations in the three major gTLDs, .com, .org and .net[27]—as new users flooded onto the Internet, it registered millions of domain names. Meanwhile, however, the very informal, consensus-driven, and perhaps unsophisticated method for creating new gTLDs broke down under the strain of competing interests. Registrars wishing to compete with NSI chafed at its contractual government monopoly and its monopolistic practices. Users who were not first to the Internet wanted new, short, domain names, and new gTLDs to register them in if the ones in the existing gTLDs (especially .com) were already taken. Trademark holders, waking up to the marketing and commercial potential of the Internet, wanted controls on the ability of others to register words that paralleled or resembled their marks. Registrants accused of cybersquatting wanted a less draconian method of dealing with such charges than NSI's policy of simply de-activating their domain name pending the slow, sometimes endlessly deferred, resolution of the dispute.

Whether there should be new top-level domain names was especially controversial. Although it is easy for the DNS system controller to create new gTLDs[28]—and indeed Dr. Postel proposed creating hundreds—intellectual property rights holders objected to additional gTLDs, arguing with some justification that they already faced mounting problems from cybersquatters—speculators who registered domain names corresponding to trademarks and sought to resell them to the trademark holders for profit.[29] Meanwhile, foreign governments, and especially the European Union (EU), began to express understandable concern about the United States's control of a critical element of a global communication and commercial resource on which they foresaw their economies and societies becoming ever-more dependent.[30]

In June, 1998, a task force headed by Senior Presidential Adviser Ira Magaziner issued a statement of policy on the *Management of Inter-*

27. *See* ELLEN RONY & PETER RONY, THE DOMAIN NAME HANDBOOK 140 (1998) (noting that NSI held monopoly of registrations in .com, .org, and .net for five years).

28. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 22 n.12.

29. *See*, *e.g.*, WORLD INTELLECTUAL PROP. ORG., FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS ¶ 23 (Apr. 30, 1999), *available at* http://wipo2.wipo.int/process1/report/finalreport.html (on file with the University of Illinois Law Review) [hereinafter WIPO FINAL REPORT] (noting the existence of "a number of predatory and parasitical practices that have been adopted by some . . . includ[ing] the deliberate, bad faith registration as domain names of well-known and other trademarks in the hope of being able to sell the domain names to the owners of those marks"). *See generally* Litman, *supra* note 3.

30. *See* Angela Proffitt, *Drop the Government, Keep the Law: New International Body for Domain Name Assignment Can Learn from United States Trademark Experience*, 19 LOY. L.A. ENT. L.J. 601, 608 (1999) (noting the concerns of the European Union, the Australian government, and others that the United States had "too much control over the DNS").

net Names and Addresses, known as the DNS White Paper.[31] The White Paper called for the government to transition its control of the DNS to a private corporation identified only as the "new corporation" (NewCo).[32] The White Paper did not actually mandate the creation of this corporation, but—nicely skirting the prohibitions of the Government Corporation Control Act (GCCA)[33]—only said how nice it would be if someone would form it to undertake certain specified tasks so that the government could strike a deal with it.[34] And, not quite fortuitously, a group of worthies did just that, forming a California non-profit corporation called ICANN, and the government duly recognized ICANN as NewCo.

ICANN's subsequent history has been fraught with controversy, but only a few facets of that history need to be related for our purposes: (1) the extent to which ICANN is controlled by the government, which is relevant to its status as a potential antitrust state actor; (2) the extent to which registries and registrars control ICANN and/or are controlled by it, which speaks to how they might be using ICANN to collude in anticompetitive conduct; and (3) three specific instances of ICANN-imposed policies which affect competition: the means by which ICANN has constrained the introduction of new TLDs, which affects competition between registries; the UDRP, which limits service competition among registrars; and ICANN's approval of VeriSign's "Waiting List Service," which eliminates competition in the market for nonrenewed domain names.

A. ICANN's Relationship with the Federal Government

ICANN is formally independent of the federal government. Its eighteen-person Board of Directors currently consists of four hold-over directors from the original nine self-selected incorporators, five directors elected in a somewhat controversial process[35] from each of five geographical world regions, and nine directors appointed by three different functional groups established by ICANN on corporatist lines.[36] Other than having anointed ICANN as its DNS representative, and thus approving the original incorporators, the U.S. government has had no formal input into the selection of ICANN's directors. Like some thirty-plus other governments, the U.S. government participates in the quarterly

31. Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 8–10, 1998) [hereinafter White Paper].

32. *Id.* at 31,751.

33. 31 U.S.C. §§ 9101–9110 (2000). The GCCA sets up a regime of audit and control for wholly owned government corporations and a looser regime for mixed-ownership government corporations. It prohibits the creation of new government corporations without explicit congressional authorization. *See* 31 U.S.C. § 9102; *see also* Froomkin, *Reinventing*, *supra* note 7, at 605–06.

34. *See* White Paper, *supra* note 31, at 31,744 (stating that "[t]he U.S. Government is committed to a transition that will allow the private sector to take leadership for DNS management").

35. *See* Weinberg, ICANN and New TLDs, *supra* note 3, at 11.

36. *Id.* There is actually a nineteenth director: the ICANN President serves *ex officio*.

meetings of ICANN's Government Advisory Committee (GAC). ICANN's rules give the GAC a right of consultation on major issues and a right to offer unsolicited advice at any time, but do not require ICANN to follow its instructions.[37]

ICANN's direct relationship with the U.S. government is defined by five elements: the White Paper, three separate government contracts, and the less formal but highly significant oversight exercised by the DoC, which recognized ICANN as the entity contemplated in the White Paper.

1. The White Paper

Although as a mere policy statement the White Paper had no direct legal force, its very vagueness on key points makes it the closest thing to a consensus document produced on DNS matters in the last five years. In June 1999, ICANN stated that the White Paper "principles . . . have dictated ICANN's policy decisions to date."[38] More recently, the DoC and ICANN's Vice President and General Counsel both reaffirmed the White Paper's centrality to DNS policy.[39] The White Paper instructed ICANN to undertake specific tasks, including fostering competition among registrars and attacking the cybersquatting issue.[40] From its creation as the body seeking to be anointed as NewCo to the present day, ICANN has assiduously undertaken to accomplish each of the specific goals set out in the White Paper.

37. ICANN, *Bylaws* art. VII, § 30(a), art. III, § 3, *available at* http://www.icann.org/general/bylaws.htm (last amended Feb. 12, 2002) (on file with the University of Illinois Law Review) ("The Governmental Advisory Committee should consider and provide advice on the activities of the Corporation as they relate to concerns of governments, particularly matters where there may be an interaction between the Corporation's policies and various laws, and international agreements. The Board will notify the chairman of the Governmental Advisory Committee of any proposal for which it seeks comments under Article III, Section 3(b) [when 'policies that are being considered by the Board for adoption that substantially affect the operation of the Internet or third parties'] and will consider any response to that notification prior to taking action.").

38. Esther Dyson & Michael M. Roberts, ICANN, *Status Report to the Department of Commerce* § I, *available at* http://www.icann.org/statusreport-15june99.htm (June 15, 1999) (on file with the University of Illinois Law Review).

39. *See* Letter from John F. Sopko, Acting Assistant Secretary for Communications and Information, to William F. Bode, Bode & Beckman, LLP (June 25, 2001), *available at* http://www.icannwatch.org/article.php?sid=237 (on file with the University of Illinois Law Review) (reiterating White Paper's "recogni[tion] that the selection of new TLDs should be conducted by the private sector through a not-for-profit organization, globally representative of the Internet stakeholder community"); *see also* Posting of Louis Touton, touton@icann.org, to council@dnso.org (July 10, 2001), *available at* http://www.dnso.org/clubpublic/council/Arc05/msg00613.html (on file with the University of Illinois Law Review).

40. It also set out four general goals for the nonprofit entity that was to manage the DNS: "stability, competition, private bottom-up coordination, and representation." *See* White Paper, *supra* note 31, at 31,743. ICANN wasted no time addressing the specific tasks in the White Paper, but some of these more general goals have proved more difficult to achieve, especially where they conflict with each other. With "stability" listed in the White Paper as "the first priority of any DNS management system," ICANN has argued that some of the other goals, notably representation, needed to take a back seat. *Id.* at 31,749.

The White Paper opined that NewCo "should be headquartered in the United States, and incorporated in the U.S. as a not-for-profit corporation. It should, however, have a board of directors from around the world."[41] ICANN complied. The White Paper said that NewCo should take over the existing IANA staff, and ICANN, with the DoC's cooperation, later did just that. NewCo, said the White Paper, should have the authority to "[s]et policy for and direct allocation of IP number blocks to regional Internet number registries" and "[o]versee operation of the authoritative Internet root server system."[42] Furthermore, NewCo would "[o]versee policy for determining the circumstances under which new TLDs are added to the root system" while coordinating "the assignment of other Internet technical parameters as needed."[43] If the DoC's contracts with ICANN did not necessarily give it this authority directly, they created the conditions in which ICANN could, with the DoC's at least tacit blessing, exercise it for all practical purposes.

The White Paper directed that NewCo require that specified information about domain name registrants be included in all registry databases and made freely available on the Internet to allow trademark holders to "contact a domain name registrant when a conflict arises between a trademark holder and a domain name holder."[44] Registrants should be required to pay fees at the time of registration, and required to "agree to submit infringing domain names to the authority of a court of law in the jurisdiction in which the registry, registry database, registrar, or the 'A' root servers are located."[45] NewCo should also require registrants to agree to arbitration in cases of alleged cybersquatting[46] and give special protections for famous trademarks.[47] With the exception of the special protection for famous marks, which foundered on an inability to agree on how to identify which marks were sufficiently famous, ICANN quickly implemented each of these directives.

The White Paper also prescribed a structure for NewCo's board of directors. The board "should be balanced to equitably represent the interests of IP number registries, domain name registries, domain name registrars, the technical community, Internet service providers (ISPs), and Internet users (commercial, not-for-profit, and individuals) from around the world,"[48] but government officials would be forbidden to

41. *Id.* at 31,750. While the White Paper itself does not use the name "NewCo," the use of the term by DoC to describe the entity called for in the White Paper dates at least from *Cooperative Agreement Between NSI and U.S. Government No. NCR-9218742, Amendment 11*, *available at* http://www.icann.org/nsi/coopagmt-amend11-07oct98.htm (Oct. 7, 1998) (on file with the University of Illinois Law Review) [hereinafter *Cooperative Agreement*].

42. White Paper, *supra* note 31, at 31,749.

43. *Id.*

44. *Id.* at 31,750.

45. *Id.*

46. *Id.*

47. *Id.* at 31,751.

48. *Id*. at 31,750.

serve on the board. The interim board would "develop policies for the addition of TLDs, and establish the qualifications for domain name registries and domain name registrars within the system."[49] ICANN faithfully followed most of these directions, although it took a long time to elect user representatives, and opinions differ on whether even today users and non-profits are equitably represented on the board.

2. The Three Contracts

Formally, the federal government administers its relationship with ICANN via three agreements: (1) a Memorandum of Understanding (MoU),[50] (2) an unusual no-cost, no-bid "procurement" contract for the "IANA function"[51] and (3) a Cooperative Research and Development Agreement (CRADA).[52]

a. Memorandum of Understanding

The MoU was the DoC's first agreement with ICANN, signed even before the DoC recognized ICANN as NewCo. The DoC and ICANN agreed to "jointly design, develop, and test the mechanisms, methods, and procedures that should be in place and the steps necessary to transition management responsibility for DNS functions now performed by, or on behalf of, the U.S. Government to a private-sector not-for-profit entity" to prepare the ground for the transition of DNS management to

49. *Id.*

50. *Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers*, *available at* http://www.icann.org/general/icann-mou-25nov98.htm (Nov. 25, 1998) (on file with the University of Illinois Law Review) [hereinafter *Memorandum of Understanding*]. The DoC renewed this agreement for a year. *See Amendment 5 to ICANN/DOC Memorandum of Understanding*, *available at* http://www.icann.org/general/amend5-jpamou-19sep02.htm (Sept. 17, 2002) (on file with the University of Illinois Law Review). However, the DoC also issued an accompanying statement making clear its displeasure with ICANN's performance, and pointedly noting that "no obvious alternative exists for long-term DNS management. Of course, if ICANN does not make significant progress on the transition tasks, alternatives will be identified and considered." Dep't Commerce, *Statement Regarding Extension of Memorandum of Understanding with ICANN* § II.E, *available at* http://www.ntia.doc.gov/ntiahome/domainname/agreements/docstatement_09192002.htm (Sept. 20, 2002) (on file with the University of Illinois Law Review) [hereinafter *Extension Statement*].

51. *Contract Between ICANN and the United States Government for Performance of the IANA Function*, *available at* http://www.icann.org/general/iana-contract-09feb00.htm (Feb. 8, 2000) (on file with the University of Illinois Law Review) [hereinafter *IANA Function Contract*] ("At the effective date of this purchase order, the Contractor shall not impose or collect any fees for performing the IANA functions under this purchase order. After the effective date of this purchase order, ICANN may establish and collect fees from third parties (i.e. other than the United States Government) for the functions performed under this purchase order, provided the fee levels are approved by the Contracting Officer before going into effect, which approval shall not be withheld unreasonably provided the fee levels are fair and equitable and provided the aggregate fees charged during the term of this purchase order do not exceed the cost of providing the functions.").

52. *Cooperative Research and Development Agreement*, *available at* http://www.icann.org/committees/dns-root/crada.htm (June 1999) (on file with the University of Illinois Law Review) [hereinafter *CRADA*].

ICANN.[53] The "DNS management functions" included oversight of both "the operation of the authoritative root server system" and "the policy for determining the circumstances under which new top-level domains would be added to the root system," plus any other agreed activities "necessary to coordinate the specified DNS management functions."[54] Echoing the White Paper, the DoC-ICANN MoU also listed four principles by which the parties "will abide:" stability of the Internet; competition; private, bottom-up coordination; and representation.[55] The MoU appears to authorize no more than a study of how the DNS would be privatized in the future. In fact, however, the DoC-ICANN MoU conveyed very significant authority, because the means by which ICANN would "study" the future privatization of the DNS was by acting as if the DNS were already privatized.[56]

A year later, the DoC and ICANN amended the MoU. ICANN promised not to amend its standard form agreement with registries without the DoC's prior approval.[57] ICANN also promised not to make agreements with a successor registry without the DoC's approval and to follow the DoC's lead if it chose to replace NSI with a new registry.[58] And most importantly, in that it gave the DoC additional leverage, ICANN agreed that "[i]f DOC withdraws its recognition of ICANN or any successor entity by terminating this MOU, ICANN agrees that it will assign to DOC any rights that ICANN has in all existing contracts with registries and registrars."[59] Whether this "termination" language would apply if the agreement were allowed to lapse instead of being actively ended by the DoC is an interesting question; the ambiguity may give ICANN leverage in any contract negotiations.[60]

53. *Memorandum of Understanding*, *supra* note 50, § II.B.

54. *Id.*

55. *Id.* § II.C.

56. As the DoC later explained to a House Committee:

> ICANN's responsibility under the [MoU] is to act as the not-for-profit entity contemplated in the White Paper, and to demonstrate whether such an entity can implement the goals of the White Paper. If it cannot, Government involvement in DNS management would likely need to be extended until such time as a reliable mechanism can be established to meet those goals. The Department does not oversee ICANN's daily operations. The Department's general oversight authority is broad, and, if necessary, the Department could terminate the agreement and ICANN's role in this aspect of DNS management with 120 days notice.

Letter from Andrew J. Pincus, General Counsel, Department of Commerce, to Rep. Tom Bliley, Chairman, United States House Committee on Commerce (July 8, 1999), *available at* http://www.ntia.doc.gov/ntiahome/domainname/blileyrsp.htm (on file with the University of Illinois Law Review).

57. *See Amendment 1 to ICANN/DOC Memorandum of Understanding*, *available at* http://www.icann.org/amend1-jpamou-04nov99.htm (Nov. 4, 1999) (on file with the University of Illinois Law Review).

58. *See id.*

59. *Id.*

60. ICANN's chief outside counsel, Joe Sims, recently argued that ICANN's authority exists independently of any delegation from the U.S. government. *See* Sims & Bauerly, *supra* note 6. One of us found that risible. *See* A. Michael Froomkin, *Form and Substance in Cyberspace*, 6 J. SMALL & EMERGING BUS. L. 93, 113–22 (2002) [hereinafter Froomkin, *Form and Substance*].

b. The IANA Procurement

The DoC issued a sole source contract to ICANN for the IANA function on the grounds that ICANN was the only responsible source available.[61] The DoC duly issued a purchase order to ICANN for IANA services, a purchase order that has a price of zero dollars but allows ICANN to establish and collect fees from third parties, subject to review by the DoC, so long as the fees reflect the actual cost of providing the service.[62]

c. The CRADA

In the ICANN-DoC MoU, the parties had agreed that ICANN would "study" the privatization of the DNS by doing it. However, IANA, a separate government contractor, was already doing the job that ICANN proposed to privatize.[63] In the June 1999 CRADA,[64] the DoC engaged ICANN to study how to improve the IANA functions. Again, like the ICANN-DoC MoU, this new agreement appears to include having ICANN perform the function during the study.[65]

61. U.S. GEN. ACCOUNTING OFFICE, GAO/OGC-OO-33A, DEP'T COMMERCE: RELATIONSHIP WITH THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS 17–19 (2000) [hereinafter GAO REPORT].

62. *See IANA Function Contract*, *supra* note 51, § 3 (showing a copy of the purchase order). The DoC later extended the "purchase order" for up to one year. *See* ICANN, *Announcement: ICANN and U.S. Government Agree to Extend Agreements*, *available at* http://www.icann.org/announcements/icann-pr04sep00.htm (Sept. 4, 2000) (on file with the University of Illinois Law Review). This extension affected both the ICANN-DoC MoU of November 25, 1998, *see Memorandum of Understanding*, *supra* note 50, and ICANN's Cooperative Research and Development Agreement. *See CRADA*, *supra* note 52.

63. A copy of what appears to be an agreement between that contractor, the University of Southern California (USC), and ICANN, dated January 1, 1999, appears as Appendix 21 to ICANN's application for tax-exempt status. *See Form 1023 (Appendix 21): USC/ICANN Transition Agreement*, *available at* http://www.icann.org/financials/tax/us/appendix-21.htm (last modified Sept. 4, 2000) (on file with the University of Illinois Law Review); *see also Form 1023 (Appendix 19): Loanout Agreement*, *available at* http://www.icann.org/financials/tax/us/appendix-19.htm (last modified Sept. 4, 2000) (on file with the University of Illinois Law Review) (detailing a loan out agreement for two employees from USC to ICANN).

64. *CRADA*, *supra* note 52. A CRADA is usually an agreement in which, as the United States Geological Survey explained:

> The collaborating partner agrees to provide funds, personnel, services, facilities, equipment or other resources needed to conduct a specific research or development effort while the Federal government agrees to provide similar resources *but not funds* directly to the partner. . . . The CRADA vehicle provides incentives that can help speed the commercialization of Federally-developed technology, making it an excellent technology transfer tool.

Technology Enterprise Office, U.S. Geological Survey, *What Is a CRADA?*, *available at* http://www.usgs.gov/tech-transfer/what-crada.html (last modified Aug. 19, 2002) (on file with the University of Illinois Law Review).

65. *See CRADA*, *supra* note 52; GAO REPORT, *supra* note 61, at 17–19.

3. Ongoing Supervision

The DoC's supervision of ICANN has three visible forms. First, the DoC's contracts with ICANN and NSI/VeriSign[66] require NSI to secure written instructions from the DoC before making changes in the root file.[67] Thus, any of ICANN's recommendations on new TLDs require at least rubber-stamp approval from the DoC. While this might be thought to provide an occasion for review, the DoC has not in fact done so. Indeed, in a June 2001 letter denying a petition for rulemaking on the subject of new gTLDs, the DoC reiterated that, following the White Paper, the DoC would as a matter of policy approve ICANN's decisions without subjecting them to review.[68]

Second, the DoC's MoU with ICANN provides for oversight and cooperation, although from the outside it often is difficult to tell how much of this there is at any given moment. ICANN sends the DoC an annual report about its performance under the MoU.[69] The DoC promised to devote more than a quarter of a million dollars in staff time[70] and expenses to monitoring and helping ICANN. The DoC's accounts of the actual intensity of this effort have varied. A DoC official testified that "[t]he Department's general oversight under the joint project is limited to ensuring that ICANN's activities are in accordance with the joint project MOU, which in turn requires ICANN to perform its MOU tasks in accordance with the White Paper."[71] But when pressed for specifics, the DoC stated that it "consults" with ICANN before its major decisions, such as ICANN's proposal to charge a fee of one dollar per domain name.[72] The DoC clearly supported ICANN during its first thirteen months by pressuring its other contractor, NSI, to recognize ICANN.[73]

66. VeriSign purchased NSI in 2000. Throughout, we use "NSI" to refer to the entity that acted before the merger, and "VeriSign" or "NSI/VeriSign" to refer to the current entity.

67. *See Cooperative Agreement*, *supra* note 41.

68. The letter stated that:

> In July 1998, the Department of Commerce made it clear that it would not participate in the selection process of new TLDs as set forth in the Statement of Policy, entitled Management of Internet Names and Addresses, 63 Fed. Reg. 31741 (1998). In the Statement of Policy, the Department recognized that the selection of new TLDs should be conducted by the private sector through a not-for-profit organization, globally representative of the Internet stakeholder community. The Department recognized ICANN as that organization in November 1998 through a Memorandum of Understanding.

Letter from John F. Sopko to William H. Bode, *supra* note 39.

69. Dyson & Roberts, *supra* note 38; ICANN, *Second Status Report Under ICANN/US Government Memorandum of Understanding*, *available at* http://www.icann.org/general/statusreport-30jun00.htm (June 30, 2000) (on file with the University of Illinois Law Review); ICANN, *Third Status Report Under ICANN/US Government Memorandum of Understanding*, *available at* http://www.icann.org/general/statusreport-03jul01.htm (July 3, 2001) (on file with the University of Illinois Law Review).

70. *See Memorandum of Understanding*, *supra* note 50, app. B (noting that the DoC promised half-time dedication of four or five full-time employees).

71. Letter from Andres J. Pincus to Rep. Tom Bliley, *supra* note 56, § E.3.

72. *See id.* § E.2; *see also* GAO REPORT, *supra* note 61, at 23 (discussing the cooperation between ICANN and DoC regarding the above-mentioned fee).

73. See, for example, the DoC's statement that:

Since then, the DoC has occasionally intervened publicly in ICANN's affairs, such as its month-long review and ultimate amendment of ICANN's proposed renegotiation of its agreement with VeriSign, undertaken after some prodding by Congress.[74] Subsequently, DoC Secretary Donald Evans wrote to ICANN urging it to approve more top-level domain names soon,[75] although it is not clear if this letter had any direct effect.

Indeed, a recent General Accounting Office (GAO) Report characterized the DoC's oversight as limited:

> [T]he Department's relationship with ICANN is limited to its agreements with the corporation, and its oversight is limited to determining whether the terms of these agreements are being met. [According to DoC officials,] the Department does not involve itself in the internal governance of ICANN, is not involved in ICANN's day-to-day operations, and would not intervene in ICANN's activities unless the corporation's actions were inconsistent with the terms of its agreements with the Department. . . . Department officials said that they carry out their oversight of ICANN's MOU-related activities mainly through ongoing informal discussions with ICANN officials. They told us that there is no formal record of these discussions.[76]

The GAO report also complained that the DoC's "public assessment of the status of the transition process has been limited in that its oversight of ICANN has been informal, it has not issued status reports, and it has not publicly commented on specific reform proposals being considered by ICANN."[77]

Perhaps the most important, but least visible, form of supervision is the sword of Damocles that the DoC holds over ICANN's head. ICANN's powers stem from its contracts, and its recognition by the DoC as the "'NewCo" specified in the White Paper. The original MoU al-

---

> Network Solutions has indicated that it is not obligated to enter into a contract with ICANN because the Department of Commerce has not "recognized" ICANN by transferring authority over the authoritative root system to it. We find no merit in this argument. The Department of Commerce entered into a Memorandum of Understanding with ICANN on November 25, 1998. That MOU constitutes the Government's "recognition" of ICANN. We reiterated this point in a letter to Network Solutions on February 26, 1999.

Letter from Andrew J. Pincus to Rep. Tom Bliley, *supra* note 56, § E.3.

74. Press Release, Dep't Commerce, Commerce Ensures Competitiveness and Stability Are Protected in New ICANN-Verisign Agreement (May 18, 2001), *reprinted in* A. Michael Froomkin, *SPIN CYCLE: Commerce Release on Final ICANN/Verisign Domain Name Registry Deal*, ICANNWATCH (May 18, 2001), *available at* http://www.icannwatch.org/article.php?sid=159 (on file with the University of Illinois Law Review) [hereinafter Froomkin, *SPIN CYCLE*].

75. Letter from Donald L. Evans, Secretary, Dep't Commerce, to Dr. Vint Cerf, Chairman, ICANN (May 25, 2001), *available at* http://www.icann.org/correspondence/doc-to-icann-25may01.htm (on file with the University of Illinois Law Review).

76. *Hearing on Internet Management: Limited Progress on Privatization Project Makes Outcome Uncertain, Before the Senate Subcomm. on Sci., Tech. & Space, Senate Comm. on Commerce, Sci. & Transp.*, 107th Cong. 12–13 (2002) [hereinafter *Hearing on Internet Management*] (statement of Peter Guerrero, Director, Physical Infrastructure Issues, U.S. Gen. Accounting Office).

77. *Id.* at 12.

lowed the DoC to terminate the agreement on September 30, 2000, or after 120 days notice, and subsequent extensions have had similar provisions.[78] As all the DoC-ICANN contracts require annual or semi-annual renewal, they provide a means for DoC to pressure ICANN were it to choose to do so. In theory, the DoC could transfer its imprimatur from ICANN to another body,[79] and some have called upon it to do just that.[80] Further, the DoC at least nominally retains policy-making authority over the legacy root,[81] though historically it has not shown much inclination to exercise that power.

Two developments, however, suggest that the DoC may be preparing to exercise more intensive oversight over ICANN. First, the GAO very strongly encouraged the DoC to issue regular public status reports about ICANN.[82] Second, the DoC accompanied its most recent renewal of ICANN's MoU with a statement emphasizing that "the Department will be closely monitoring ICANN's efforts, particularly through a quarterly reporting mechanism, and expects to see significant advancement" during this "critical period for ICANN to make substantial progress on the remaining transition tasks."[83]

B. Structural Relationships Among ICANN, Registries, Registrars, and Alternate Roots

Adhering, more or less, to the White Paper's directions regarding the internal organization of NewCo,[84] ICANN created three subsidiary councils charged with developing policy and making recommendations to the board. Each of these three groups also elected three of the ICANN board's eighteen directors. One of these three bodies, the Domain Name Supporting Organization (DNSO) is charged with concentrating on domain name related issues. The DNSO gives registrars (and, now that

78. *See Memorandum of Understanding*, *supra* note 50, § VII.

79. As we write this, ICANN is currently engaged in a reform process that is likely to result in some changes to its structure. An initial proposal to have governments select a third of the ICANN Board, *see* Lynn, *supra* note 4, appears to have been abandoned. While the other changes being discussed will likely have substantial implications for ICANN legitimacy and efficiency, the only effects these changes are likely to have on the arguments presented here is that they may change the balance of power on the ICANN board. *See supra* note 16 and accompanying text. To what extent the composition of the board defines outcomes, and to what extent the real power is exerted by the staff, are disputed questions. *See, e.g.*, David R. Johnson & Susan P. Crawford, *ICANN 2.0*, ICANNWATCH (Feb. 26, 2002), *available at* http://www.icannwatch.org/essays/022602-johnson-crawford-icann2.htm (on file with the University of Illinois Law Review) (noting argument).

80. *See, e.g.*, Media Access Project, Non-Profits Urge Department of Commerce: Select Internet Address Manager Through Open Competition (May 29, 2002), *reprinted in* A. Michael Froomkin, *NGOs to DoC: Rebid!*, ICANNWATCH (May 29, 2002), *available at* http://www.icannwatch.org/article.php?sid=772 (on file with the University of Illinois Law Review).

81. *See* MILTON L. MUELLER, RULING THE ROOT 197 (2002).

82. *See Hearing on Internet Management*, *supra* note 76, at 15–16 (statement of Peter Guerrero, GAO).

83. *See Extension Statement*, *supra* note 50, § I.

84. *See* White Paper, *supra* note 31, at 31,744.

there are more than one, gTLD registries) a place to meet, to lobby ICANN, and to exert some influence on the selection of its directors.

The DNSO is subdivided into seven 'stakeholder' constituencies selected by the nine initial self-selected ICANN directors: registrars,[85] gTLD registries, ccTLDs, ISPs, trademark holders, businesses, and noncommercial domain name holders.[86] Each of the seven constituencies elects three[87] representatives to the DNSO's governing body, the Names Council, which in turn elects three representatives to the ICANN board. The registrars' strength may be greater than it seems, however, since registrars could join more than one constituency simultaneously. Indeed, a single firm could simultaneously be a member of at least three: ISP and connectivity providers; registrars; and trademark, other intellectual property, and anticounterfeiting interests.[88]

ICANN has substantial power over registrars, as its nonnegotiable standard form Registrar Agreement requires them to pledge to observe ICANN's policy decisions[89] and also gives ICANN the power to disqualify a registrar.[90] gTLD Registries must make a similar pledge to follow ICANN's consensus policies. As the new gTLD's contracts are each unique, ICANN is able to impose additional requirements on them before allowing them to join the legacy root. ICANN's control does not (yet) extend to any but a few of the ccTLD registries, although ICANN is

85. Originally, future registrars were allowed to enter the registrars' constituency and vote before they were accredited by ICANN, but future registries were not. Today, however, only ICANN-accredited registrars may join the Registrars Constituency. *See* ICANN-Accredited Registrars' Constituency, *The DNSO Registrar Constituency By-laws* § 2.1, *available at* http://www.icann-registrars.org/pdfs/bylaws1.pdf (Oct. 9, 2001) (on file with the University of Illinois Law Review).

86. The seven constituencies official names are: ccTLD registries; commercial and business entities; gTLD registries; ISP and connectivity providers; noncommercial domain name holders; registrars; and trademark, other intellectual property, and anticounterfeiting interests. *See* Domain Name Supporting Organization, *About DNSO*, *available at* http://www.dnso.org/dnso/aboutdnso.html (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review); *cf.* Weinberg, *Problem of Legitimacy*, *supra* note 3, at 238 n.261.

87. ICANN stripped one of the seven DNSO constituencies, the gTLD constituency, of two of its three Names Council Representatives because there was only one firm, NSI/VeriSign, represented in the constituency. The full three-member representation is due to be restored when new gTLD registries join the constituency.

88. *See* Intellectual Property Constituency, *By-Laws* § III, *available at* http://ipc.songbird.com/IPCBylaws.htm (Nov. 1, 2000) (on file with the University of Illinois Law Review); Commercial and Business Entities Constituency, *Charter* § II.A, *available at* http://www.icann.org/dnso/bussdraft2.htm (May 5, 1999) (on file with the University of Illinois Law Review); Domain Name Supporting Organization, *The DNSO Registrar Constituency* § II, *available at* http://www.dnso.org/constituency/registrars/Registrars.Articles.html (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review); Domain Name Supporting Organization, *ISPs and Connectivity Providers, How to Become a Member*, *available at* http://www.dnso.org/constituency/ispcp/membership.html (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review). The Business Constituency By-Laws prohibit registrars and registries from joining.

89. ICANN, *Registrar Accreditation Agreement* § II.J.1, *available at* http://www.icann.org/nsi/icann-raa-04nov99.htm (Nov. 4, 1999) (on file with the University of Illinois Law Review) [hereinafter *Registrar Accreditation Agreement*].

90. ICANN, *Statement of Registrar Accreditation Policy* § II.C., *available at* http://web.archive.org/web/20011127185232/http://www.icann.org/policy_statement.html (Mar. 4, 1999) (on file with the University of Illinois Law Review) [hereinafter *Registrar Accreditation Policy*].

currently negotiating agreements with them as well.[91] The ccTLDs in turn argue that because they are being asked to pay a substantial fraction of ICANN's costs, they should have direct and substantial representation on the ICANN board.[92]

ICANN's control over the registrars stems in part from its agreements with the registries. In particular, ICANN's agreement with NSI, the monopoly gTLD registry until the introduction of .biz, .info, and other new gTLDs, requires NSI to ensure that registrars accept ICANN's standard form Registrar Agreement, before allowing them to register any names.[93] And the chief "consensus" policy grandfathered into the NSI Registry Agreement (and thus exempted from the need to demonstrate consensus) is ICANN's mandatory arbitration clause for domain name disputes, the UDRP.[94]

This hierarchical relationship is complicated by the existence of "alternate" or competitive roots. Understanding alternate roots requires a short detour into DNS architecture. Recall that ICANN gets its power from its control over a key Internet chokepoint—the content of the legacy root file. Users can try to avoid the effects of this chokepoint by using so-called alternate roots. Rather than getting their name resolution service from a member of the legacy root hierarchy, users of an alternate root instead get DNS service from someone else who gets her data from a different root file with more or different entries.

91. ICANN signed its first agreement with a ccTLD on October 25, 2001. *See* ICANN, ccTLD Agreement Signed with auDA (Oct. 25, 2001), *available at* http://www.icann.org/announcements/announcement-25oct01.htm (on file with the University of Illinois Law Review). The agreement with the Australian registry operator for .au followed closely on the heels of ICANN's controversial decision to take the .au authority away from the long-time Internet pioneer who had operated it (somewhat autocratically) as a public service and transfer it to an Australian government-endorsed nonprofit entity modeled closely on ICANN itself. *See* A. Michael Froomkin, *How ICANN Policy Is Made (II)*, ICANNWATCH (Sept. 5, 2001), *available at* http://www.icannwatch.org/article.php?sid=336 (on file with the University of Illinois Law Review); A. Michael Froomkin, *The Other Shoe Drops*, ICANNWATCH (Sept. 5, 2001), *available at* http://www.icannwatch.org/article.php?sid=339 (on file with the University of Illinois Law Review). ICANN has also entered into agreements with the registries for .bi (Burundi, May 2002), .jp (Japan, February 2002) and .mw (Malawi, June 2002). *See* ICANN, *ICANN's Major Agreements and Related Reports*, *available at* http://www.icann.org/general/agreements.htm (last modified Aug. 16, 2002) (on file with the University of Illinois Law Review) [hereinafter ICANN, *Major Agreements*].

92. *See, e.g.*, ccTLD Constituency, Communiqué presented to the ICANN Public Forum in Accra, Ghana (Mar. 13, 2002), *available at* http://www.wwtld.org/communiqué/ccTLDGhana_communique_13Mar2002.html (on file with the University of Illinois Law Review). Interestingly, ICANN itself seems sensitive to the antitrust aspects of its relationship with the ccTLDs. *See* Fay Howard, CENTR, *Legal & Regulatory Report for 9th General Assembly*, *available at* http://www.centr.org/meetings/ga-9/legal-report.html (Feb. 10, 2001) (on file with the University of Illinois Law Review) (summarizing remarks of ICANN staff member as wanting "[a]voidance of the term 'Contract for Services' to avoid scrutiny under Anti-trust regulations in the USA"). ICANN's current reform proposal would give ccTLDs two seats on the board. *See supra* note 16 and accompanying text.

93. *See ICANN-NSI Registry Agreement*, *available at* http://www.icann.org/nsi/nsi-registry-agreement-04nov99.htm (Nov. 4, 1999) (on file with the University of Illinois Law Review); *Registrar Accreditation Agreement*, *supra* note 89.

94. *Registrar Accreditation Agreement*, *supra* note 89, §§ II.K, II.P.

At the time ICANN was choosing among the applicants for new gTLDs, the most commonly deployed alternate roots were super-sets of the legacy root.[95] These alternate DNS services[96] directly or indirectly access the legacy root when users seek to resolve a domain name in, say, .com. But where legacy root servers would give an error message for lighting.faq or law.web, these services send the queries to private registries that operate without the DoC's imprimatur. Most of the alternate roots in operation belong to a loose cooperative network that works on first-come-first-served principles. This cooperative encourages peering and minimizes, but does not entirely eliminate,[97] the problem of "colliders"—two or more registries claiming to be the authoritative source of registrations in a particular TLD.[98]

An interesting variant on an alternate root is New.net. New.net is both more and less than a true alternate root, and is perhaps the most visible competitor for namespace with ICANN.[99] New.net markets itself as a source of domains in thirty new English-language TLDs with names such as .shop, .kids, .law, .xxx, plus a large number of attractive Spanish, French and Portuguese TLDs.[100]

The registrant of, say, kafka.law at New.net actually receives a dual registration. In addition to receiving kafka.law in the New.net DNS, she also receives a registration of kafka.law.new.net in the legacy root—a fourth-level sub-domain of New.net. Since New.net's .law domain is not in the legacy root, most Internet users worldwide who attempt to access kafka.law will get an error message. New.net attempts to overcome this, and simulate a genuine legacy TLD, by using a combination of two strategies, one aimed at ISPs and one aimed at users. New.net invites (and perhaps even compensates) ISPs to alter their DNS to include

95. A subsequent entrant to the non-ICANN domain name market actually offers a service that is a complex blend of legacy and alternate root services. *See infra* notes 99–105 and accompanying text (discussing New.net).

96. The leading alternate root providers are loosely allied under the umbrella of the Open Root Server Confederation (ORSC). ORSC's homepage is available at http://www.open-rsc.org (last visited Oct. 8, 2002).

97. For an example of an alternate root operator who runs colliding TLDs, see Sarah Ferguson, *Casting a Wider Net*, VILLAGE VOICE (Apr. 10, 2001) (profiling Paul Garrin of Name.space), *available at* http://www.villagevoice.com/issues/0114/ferguson.php (on file with the University of Illinois Law Review).

98. Until now there have been no alternate roots open to the public that carry data conflicting with the legacy root. Thus, when a user of an alternate root types a name in .com, .edu or .uk, that user gets the same IP number as does a user of the legacy root. However, the recent introduction of a .biz TLD may change that. Many of the existing alternate roots use a root file that points to a small .biz registry operated by Atlantic Root Network, http://www.biztld.net/. If they persist in doing so after the ICANN-sponsored .biz goes live, the supersets will become conflicting sets.

99. On the growth of New.net, see Chris Gaither, *New Challenge to Domain Name Registry*, N.Y. TIMES, May 15, 2001, at C12 (noting that Prodigy now supports New.net); May Wong, *Rebel Registry Adds 20 Domain Name Extensions*, S.F. CHRON., Mar. 6, 2001, at C3.

100. *See* New.net, *Guiding Principles*, *available at* http://www.new.net/about_us_guiding.tp (last visited Aug. 21, 2002) (on file with the University of Illinois Law Review).

New.net's TLDs.[101] New.net claims it has agreements with ISPs with more than 132 million users,[102] a significant number, but only a fraction of the more than 580 million estimated Internet users worldwide.[103] For everyone else, New.net offers a "plug-in" program that users of popular browsers can install on their computers.[104] Once this program is installed, it intercepts attempts to access any New.net TLD (or to email to a New.net address) and adds the "new.net" extension as needed. Thus, users of the plug-in and customers of participating ISPs can browse both the legacy namespace and the New.net namespace at will. For them, www.kafka.law will resolve, and mail to kafka.law will reach its destination (albeit as kafka.law.new.net in some cases). Difficulties start, however, when the holder of the kafka.law registration wants to have a person who neither has a participating ISP nor the plug-in write back or visit her new web site. They must either type the full legacy address of kafka.law.new.net—which more or less defeats the purpose of having the catchy name in the first place—or be induced to get the plug-in.[105] And if they use a browser or operating system for which there is no plug-in, even that is not an option. Obviously, New.net is hoping to break through the network effect and get more people to become part of its network. Equally obviously, it has yet to work: you do not see New.net TLDs on business cards.

C. ICANN Policies with Competitive Implications

1. Constrained Roll-Out of New TLDs

ICANN selected the first seven new gTLDs for inclusion in the legacy root at its second annual meeting in Los Angeles from a crowded and highly contentious field of forty seven applicants, each of whom had paid a non-refundable $50,000 application fee.[106] In one sense, the November

101. *See* New.net, *ISP Information*, *available at* http://www.new.net/help_isp_info.tp (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review); Posting of Aaron Hopkins, Acting VP of Engineering, New.net, to North American Network Operators Group (Mar. 7, 2001), *available at* http://www.merit.edu/mail.archives/html/nanog/2001-03/msg00136.html (on file with the University of Illinois Law Review).

102. *See* New.net, *New.net Is Growing Fast*, *available at* http://www.new.net (last visited Aug. 21, 2002) (on file with the University of Illinois Law Review).

103. *See* Nua.com, *How Many Online?*, *available at* http://www.nua.ie/surveys/how_many_online/index.html (on file with the University of Illinois Law Review) ("educated guess" as of May 2002).

104. An early version of the plug-in, however, caused crashes on some computers. *See* Bugtoaster, *Resolution #98*, *available at* http://www.bugtoaster.com/dw15/Reports/ResolutionDetail.asp?DefectID=98 (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review).

105. *See* New.net, *FAQ: "Can I Use My New.net Domain Names for E-Mail?"*, *available at* http://www.new.net/help_faq.tp1 (last visited Aug. 22, 2002) (on file with the University of Illinois Law Review).

106. ICANN, *Second Annual Meeting and Organizational Meetings of the ICANN Board*, *available at* http://www.icann.org/minutes/prelim-report-16nov00.htm (Nov. 16, 2000) (on file with the University of Illinois Law Review). The selected TLD proposals are of two types. Four proposals (.biz, .info, .name, and .pro) are for relatively large, "unsponsored" TLDs. The other three proposals (.aero, .coop, and .museum) are for smaller, "sponsored" TLDs. Generally speaking, an "unsponsored" TLD

2000 decision was the culmination of almost two years of effort; in another, it was only the start of an additional two years of tough bargaining over the contract terms that would bind each registry to ICANN. ICANN signed the first new gTLD contracts in May 2001, but reached agreement with the last of the seven, .pro, in May 2002, some eighteen months after initially approving the registry.[107] After each contract was painstakingly negotiated, ICANN submitted the gTLD to the DoC. Approvals happened within a few hours of the submission, suggesting that the DoC's review was somewhat cursory.[108]

Breaking the logjam that had prevented any new gTLDs from joining the root[109] was of course one of the main reasons why the DoC wanted ICANN to exist, and why it contracted with ICANN. ICANN's internal processes leading up to the selection of new gTLDs reflected the divisions in the various affected communities, the details of which need not concern us here. At no time prior to its decision to approve only a limited number of new TLDs did ICANN issue an opinion explaining the technical justification for this (or any other) limit. Nor did ICANN refer to such a report by anyone else. In fact, so far as we can discern, no such study, report, or analysis exists. ICANN's decision was fundamentally political: an ICANN working group brokered a deal between the faction that wanted a very large number of new TLDs and those who wanted none. In April 1999, the DNSO Names Council voted to "recommend to the Board that a limited number of new top-level domains be introduced initially and that the future introduction of additional top-level domains be done only after careful evaluation of the initial introduction."[110] In so doing, it endorsed the recommendation of that Working Group, which had compromised on "six to ten, followed by an evaluation period."[111]

ICANN's decision to limit the number of new gTLDs to well below the lowest estimates of what the DNS could handle prevented greater

operates under policies established by the global Internet community directly through the ICANN process, while a "sponsored" TLD is a specialized TLD that has a sponsoring organization representing the narrower community that is most affected by the TLD. *See* ICANN, *New TLD Program*, *available at* http://www.icann.org/tlds/ (last modified July 18, 2002) (on file with the University of Illinois Law Review).

107. *See* ICANN, *Major Agreements*, *supra* note 91.

108. *See* A. Michael Froomkin, *Commerce Dept. Wields Domain Name Rubber Stamp in Record Time*, ICANNWATCH (June 26, 2001), *available at* http://www.icannwatch.org/article.php?sid=222 (on file with the University of Illinois Law Review); *see also supra* note 68 and accompanying text (discussing DoC letter explaining that it follows White Paper in leaving gTLD decisions to ICANN).

109. In contrast to gTLDs, adding ccTLDs appeared to be uncontroversial. For example, pursuant to ICANN's recommendation, the DoC authorized the creation of the .ps. ccTLD. *See* IANA, *Report on Request for Delegation of the .ps Top-Level Domain*, *available at* http://www.icann.org/general/ps-report-22mar00.htm (Mar. 22, 2000) (on file with the University of Illinois Law Review).

110. ICANN, *Yokohama Meeting Topic: Introduction of New Top-Level Domains* § I.C., *available at* http://www.icann.org/yokohama/new-tld-topic.htm (June 13, 2000) (on file with the University of Illinois Law Review) [hereinafter ICANN, *Yokohama Meeting*].

111. Working Group C, ICANN, *Report (Part One): (New gTLDs) Presented to Names Council*, *available at* http://www.icann.org/dnso/wgc-report-21mar00.htm (Mar. 21, 2000) (on file with the University of Illinois Law Review).

competition between registries.[112] ICANN justified its decision on the grounds of compromise, but also on the grounds that it had been a long time since a new gTLD had been introduced, and there might therefore be Internet "stability" issues to consider that required a "test" or "proof of concept" period.[113] It is unclear if this was intended as a technical claim or if, as seems more likely, the "stability" at issue was commercial or political. If the claim was based on a technical rationale, it was implausible, since several new ccTLDs had been introduced without any noticeable effect on anyone.[114] Furthermore, there can be no doubt that the method ICANN chose to select the TLDs substantially reduced competition in other ways that had no technical justification.[115] Among these were ICANN's decision to require a non-refundable $50,000 "application fee," ICANN's requirement that successful applicants demonstrate huge financial reserves; ICANN's decision to have most new TLDs limited by restrictive charters rather than being able to sell domains to all comers; and ICANN's decision to select the names of the new gTLDs itself rather than letting the winners do it on the basis of their market research.

There were, however, two ways in which the introduction of new gTLDs genuinely would be new. First, there was a huge pent-up demand for "good" domain names, leading to fears of a chaotic "landrush" period in the early moments of any new registry. Second, there was a heightened sensitivity to the concerns of trademark holders who believed not only that that they should be protected from a fresh round of cybersquatting, but that trademark owners ought to be first in the queue for new names.[116] ICANN justified the small number of gTLDs as a cautious reaction to uncertainty in light of the Internet's vastly increased size and

112. As Milton Mueller put it, "[t]he most striking feature of the ICANN regime is its perpetuation of scarcity at the top level of the name space." MUELLER, *supra* note 81, at 255. ICANN's ability to choose which TLDs would be approved also means that the "best" or most popular TLDs are not necessarily the ones ICANN will choose. Indeed, the initial TLDs chosen—what one might call the "not-so-magnificent seven"—include TLDs like .museum, .coop, and .aero which are likely to be of only minor interest.

113. *See* ICANN, *ICANN Yokohama Meeting, supra* note 110, § II.A.

114. For example, ICANN added .ps (for Palestine) to the root in March 2000. *See* IANA, *supra* note 109.

115. *See* ICANN, *Criteria for Assessing TLD Proposals*, *available at* http://www.icann.org/tlds/tld-criteria-15aug00.htm (Aug. 15, 2000) (on file with the University of Illinois Law Review) [hereinafter *Assessing TLD Proposals*]; ICANN, *New TLD Application Instructions*, *available at* http://www.icann.org/tlds/new-tld-application-instructions-15aug00.htm (last modified Sept. 1, 2000) (on file with the University of Illinois Law Review) [hereinafter *TLD Application Instructions*].

116. ICANN was not convinced by the argument, advanced by some, *see, e.g.*, A. Michael Froomkin, *Speculative Frenzy for New Domain Names Begins*, ICANNWATCH (Apr. 30, 2001), *available at* http://www.icannwatch.org/article.php?sid=133 (on file with the University of Illinois Law Review) (noting argument), that the decision to introduce only a small number of new gTLDs and to make no promises about when, if ever, there would be more actually increased the likelihood of cybersquatting, because it failed to increase the supply of new names to the point where there was no likelihood of profit from hoarding.

commercial importance,[117] a view that echoed the policy direction in the White Paper.[118]

If the initial roll-out was a "test," ICANN has been curiously slow about analyzing the data it produced. In June 2001, the ICANN board resolved to study the creation of these new gTLDs by creating "a plan for monitoring the introduction of new TLDs and for evaluating their performance and their impact on the performance of the DNS."[119] The Task Force charged with this report did not rush toward a conclusion. As of July 2002, it was still "formulating its approach to its charter and the processes it will be following."[120] When it suddenly issued its final report at the end of July 2002, one of its main recommendations was that a detailed study was needed,[121] which it recognized could greatly delay the introduction of any new gTLDs. There is currently no timetable for the introduction of further new gTLDs, nor even a timetable for the dis-

117. Probably the clearest, and yet very carefully nuanced, statement of this view came after the fact from Vinton Cerf:

> Of course, it cannot be stressed enough that no one knows for sure what the effects of this experiment will be. Since there have been no new global TLDs introduced for more than a decade, the Internet is a vastly different space than it was the last time this happened. Of course, there have been a number of country code TLDs introduced over that period, and since some of those have recently begun to function in a way quite analogous to a global TLD, it may be that we will be able to conclude that the DNS can readily absorb more new global TLDs. But there has never been an introduction of as many as seven new global TLDs simultaneously, with the possibility of a land rush that is inherent in that fact. There has never been a highly visible introduction of multiple new TLDs in the context of an Internet that has become a principal global medium for commerce and communication. We do not know whether the introduction of a number of new TLDs—especially combined with the relatively new phenomenon of the use of ccTLDs in a fashion never intended (after all, .tv stands for Tuvalu, not television, no matter what its marketers say)—will create consumer confusion, or will impair the functioning of various kinds of software that has been written to assume that .com is the most likely domain for any address.
>
> In short, it is not absolutely clear what effects these introductions will have on the stability of the DNS or how to introduce new TLDs in a way that minimizes harmful side-effects, and that is precisely why we are conducting this experiment. The results will guide our future actions.

Hearing on Internet Domain Names Before the House Comm. on Energy & Commerce, Subcomm. on Telecomm. & the Internet, 106th Cong. (2000) [hereinafter *Hearing on Domain Names*] (testimony of Dr. Vinton G. Cerf, Chairman, ICANN), 2001 WL 2005249 (on file with the University of Illinois Law Review).

118. At least in the short run, a prudent concern for the stability of the system suggests that expansion of gTLDs proceed at a deliberate and controlled pace to allow for evaluation of the impact of the new gTLDs and well-reasoned evolution of the domain space. New top level domains could be created to enhance competition and to enable the new corporation to evaluate the functioning, in the new environment, of the root server system and the software systems that enable shared registration.

White Paper, *supra* note 31, at 31,746.

119. *See* ICANN, *Preliminary Report, Meeting of the ICANN Board in Stockholm*, Resolution 1.74, *available at* http://www.icann.org/minutes/prelim-report-04jun01.htm (June 4, 2001) (on file with the University of Illinois Law Review).

120. ICANN, *New TLD Evaluation Process Planning Task Force*, *available at* http://www.icann.org/committees/ntepptf/ (last modified July 31, 2002) (on file with the University of Illinois Law Review).

121. *See* ICANN, *Final Report of the New TLD Evaluation Process Planning Task Force* § I, *available at* http://www.icann.org/committees/ntepptf/final-report-31jul02.htm (July 31, 2002) (on file with the University of Illinois Law Review) (noting that "[a] complete evaluation of the new gTLDs is a formidable undertaking that could stretch out indefinitely and could be extraordinarily expensive. The Task Force has already significantly pared down its initial list of questions and concerns, but there remains a considerable body of work. In its entirety, this may well be beyond the resources of ICANN to carry out").

cussion of a process that might lead to consideration of the *possible* introduction of new gTLDs, although the Task Force did suggest that the ICANN board might wish to consider making a timetable, and try to run some activities in parallel with its study to reduce what would otherwise be a very long delay.[122] As John Klensin, one of the most respected Internet architects, remarked in the context of the debate over who should manage the .org domain, ICANN's approach to change has the effect of restricting competition. Indeed, Klensin suggests that ICANN's behavior too frequently resembles that of the much-criticized telephone monopolies.[123]

2. Uniform Dispute Resolution Policy

The White Paper recommended that NewCo require registrants to agree "that in cases involving cyberpiracy or cybersquatting (as opposed to conflicts between legitimate competing rights holders), they would submit to and be bound by alternative dispute resolution systems identified by the new corporation for the purpose of resolving those conflicts."[124] The White Paper itself said little about what this dispute resolution policy should look like, choosing instead to ask the World Intellectual Property Organization (WIPO) to advise NewCo on a plan. The WIPO duly did just that,[125] and once it had the WIPO's advisory report in hand, ICANN wasted no time in starting its cumbersome policy-making machinery to address this issue. A "working group" was formed to consider the issues, and eventually recommended that some sort of WIPO-like policy was appropriate.[126]

Meanwhile, however, the registrars became impatient with the slow progress of the working group process. In 1999, ICANN had begun ac-

122. *See id.* § IV.

123. It appears to me that the ICANN review processes are biased, in several ways (some discussed more below), toward "only incumbent operators need apply." Spreading TLDs out among an oligarchy of existing TLD operators who are interlinked by investments, closed cross-licensing of technology, partnerships in other businesses, etc., does not strike me as the same thing as increasing competition and diversity. . . . The easy way to do a technical evaluation is to assume that only those who are already doing a given job, and doing it well, are qualified to do that job. That approach has several flaws if one is trying to, e.g., expand the number of actors in a particular area. Those of us who were around in the early days of the Internet, and involved in discussions related to the OSI model, cannot help noting that if this "only the incumbents are qualified" assumption had been applied at that time, it is likely that only then-main-line telcos would have been allowed to enter the data-network market. It [sic] that had occurred, the Internet as we know it today would probably not exist.

Posting of John C. Klensin, *Second-Guessing the ORG Process*, to org-eval@icann.org (Aug. 29, 2002), *available at* http://forum.icann.org/org-eval/preliminary-report/msg00006.html (on file with the University of Illinois Law Review).

124. White Paper, *supra* note 31, at 31,750.

125. WIPO FINAL REPORT, *supra* note 29.

126. *Cf.* A. Michael Froomkin, *Comments on ICANN Uniform Dispute Policy: A Catalog of Critical Process Failures; Progress on Substance; More Work Needed*, *available at* http://www.law.miami.edu/~amf/icann-udp.htm (Oct. 13, 1999) (on file with the University of Illinois Law Review) (critiquing operation of an early Working Group).

crediting new registrars that wished to compete with NSI. Although ICANN initially proposed a fairly detailed intellectual property protection regime,[127] in March 1999, the board adopted a policy that mostly put the question off until it decided what it should do with the WIPO's recommendations.[128]

As they prepared to go live in the so-called testbed phase in mid-1999, the newly accredited registrars found themselves in a delicate position. On the one hand, the trademark interests were telling them that they faced exposure to liability if they failed to institute some method of protecting trademark holders against cybersquatters. On the other hand, the policy then used by NSI was obviously draconian and unfair.[129] The registrars, perhaps with ICANN's encouragement, decided to draft their own dispute policy. By May 1999, the ICANN staff reported to the board that:

> the [Registrar Accreditation] Agreement calls for registrars to adopt dispute resolution policies, and that accredited registrars are already working together to do so. Counsel noted that Network Solutions' registry-registrar contract also calls for registrars to have dispute resolution policies in place, and that registrars are anxious to have guidance on a uniform policy.[130]

The registrars' desire to have a tough and uniform policy was exacerbated by political and competitive factors. By the time the new registrars entered the scene, the conventional wisdom increasingly was that "the best names are taken." The registrars as a group were therefore desperately anxious to have new product to sell—registrations in new

127. In the Proposed Accreditation Guidelines for Registrars, ICANN stated that the final document

> should protect legal rights (including intellectual property rights) of the parties, and of third parties where applicable. It should contain provisions that minimize disputes over rights to use of particular domain names, and in the event of dispute, it should contain provisions that enhance the orderly and timely resolution of disputes.

ICANN, *Proposed Guidelines for Accreditation of Internal Domain Name Registrars and for the Selection of Registrars for the Shared Registry System Testbed for .com, .net. and .org domains* § I.D.3, *available at* http://www.icann.org/singapore/draftguidelines.htm (Feb. 8, 1999) (on file with the University of Illinois Law Review). Section K of this document also contained a list of WIPO recommendations that ICANN thought should be incorporated into the Registries' practices. *Id.* § K.

128. The policy stated that:

> During the term of the accreditation agreement, the registrar will have in place a policy and procedure for resolution of disputes concerning SLD names. In the event that ICANN establishes a policy or procedure for resolution of disputes concerning SLD names that by its terms applies to the registrar, the registrar will adhere to the policy or procedure.

Registrar Accreditation Policy, *supra* note 90, § III.K. This clause became § III.J. of the *Registrar Accreditation Agreement*, *supra* note 89.

129. *See* Carl Oppedahl, *Remedies in Domain Name Lawsuits: How Is a Domain Name Like a Cow?*, 15 J. MARSHALL J. COMPUTER & INFO. L. 437, 448–50 (1997) (discussing the old policy and its problems). Under the old policy, NSI automatically put a domain name "on hold" if a trademark owner complained until the dispute was resolved. Domain name owners could therefore lose the use of their address for a substantial period of time even if the complaints against them were frivolous.

130. ICANN, *Minutes, Meeting of the Initial Board: World Intellectual Property Organization Recommendations*, *available at* http://www.icann.org/minutes/berlinminutes.html (May 27, 1999) (on file with the University of Illinois Law Review).

gTLDs in which they would be competing more evenly with NSI. They also believed—not without reason—that trademark owners had a virtual veto over the creation of new gTLDs, and that they would exercise it until they were satisfied by the intellectual property protections instituted by the registrars. This created a powerful incentive to draft a tough policy on cybersquatting to placate the trademark owners.

Tough was not enough. To satisfy the trademark interests, the policy also had to be uniform—to apply to all accredited registrars and all gTLD registrants. Indeed, the registrars themselves had a vested interest in ensuring that the policy applied to all their competitors, and especially their competitors' customers, lest some registrars compete on service terms and attract disproportionate business by being "registrant friendly"—or worse, "cybersquatter friendly." This fear was far from academic, as prior to ICANN's UDRP, different registrars had a variety of policies in place.[131]

Even before the first ICANN working group on domain name arbitration reported in late July 1999,[132] a group of registrars[133] assisted by a Skadden Arps lawyer, Rita Rodin, crafted a joint dispute policy. On August 20, 1999, the registrars unveiled their proposed policy document.[134] Four days later, the ICANN staff issued a report with its own detailed suggestions about what the dispute policy should look like, many of which followed the registrars' lead.[135] Two days after that, amidst much controversy, the ICANN board resolved to use the registrars' draft, rather than anything drafted through the ICANN consensus policymaking procedure, "as a starting point" for the drafting of

131. *See Domain Revocation Policies of ICANN Accredited Registrars*, DOMAIN NAME HANDBOOK, *available at* http://www.domainhandbook.com/dompol.html (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review). As NSI was the registry, they were all de facto subject to its policies, although there was a legal question as to liability for NSI's actions in the absence of privity with the customer.

132. *See* Working Group A, Domain Name Supporting Org., *Final Report to the Names Council, Revised Draft*, *available at* http://www.dnso.org/dnso/notes/19990729.WGA-report.html (July 29, 1999) (on file with the University of Illinois Law Review).

133. By August 1999, the group of registrars cooperating in drafting a domain name arbitration policy apparently included Alabanza, AOL, AT&T, AITcom, CORE, Domainbank, FICPI, Infonetworks, Interq-Japan, Netnames, NSI, PSI Japan, Register.com, plus the ICC and INTA. *See* Alabanza, Inc. et al., *Policy Statement Regarding the Model Domain Name Dispute Policy*, *available at* http://www.dnso.org/constituency/registrars/Website/udrp-draft-19990909.html (Sept. 9, 1999) (on file with the University of Illinois Law Review) (draft proposal). The official Registrars' Statement offered a slightly different list of Participating Registrars: Alabanza, Inc., America Online Incorporated, Animus Communications, Inc., Domain Bank, Inc., EnetRegistry.com Corporation, eNOM, Inc., InfoNetworks, Inc., Melbourne IT, Network Solutions, Inc., Nominalia Internet S.L., register.com, Tech Dogs, Inc., TUCOWS.com, Inc., and WebTrends Corporation. Alabanza, Inc. et al., *Registrars' Statement Regarding Their Model Uniform Dispute Policy*, *available at* http://www.icann.org/santiago/registrar-policy-statement.htm (Aug. 20, 1999) (on file with the University of Illinois Law Review).

134. The Registrars' policy was unveiled on August 20, and voted on by the ICANN Board at its August 24–26 meeting. *See* ICANN, *Staff Report: Uniform Dispute Resolution Policy for gTLD Registrars*, *available at* http://www.icann.org/santiago/udrp-staff-report.htm (Aug. 24, 1999) (on file with the University of Illinois Law Review).

135. *Id.*

ICANN's own policy.[136] In practice this meant that the registrars' draft was accepted almost in toto, save that a few of the most controversial issues were referred to a "small drafting committee" made up of representatives of the warring factions.[137] This committee was only advisory,[138] and the staff did not accept all of its suggestions even when it was able to reach consensus. Ultimately, the ICANN staff prepared the final draft of the UDRP, a text that owed a great deal to the registrars' draft, which in turn relied on some of the WIPO's suggestions.[139]

These facts relating to dispute resolution and constraining new TLDs have competitive significance, as we will see in part III. ICANN and those who lobby it have engaged in some conduct that may raise antitrust eyebrows. But the competitive impact of these acts matters only if ICANN is in fact subject to antitrust scrutiny at all. Hence, in part II we consider the possibility that ICANN is immune from antitrust liability for the acts we have described.

136. *See* ICANN, *Resolutions Approved by the Board, Santiago Meeting*, Resolution 99.8(1), *available at* http://www.icann.org/santiago/santiago-resolutions.htm (Aug. 26, 1999) (on file with the University of Illinois Law Review).

137. The Board resolution, *id.* at 99.82–.83, stated:

> FURTHER RESOLVED [99.82] that the President is directed, with the assistance of ICANN staff and counsel, to prepare implementation documents for approval by the Board after public notice and comment, on a schedule that allows the policy to be put into place within 45 days.
>
> FURTHER RESOLVED [99.83] that the Board gives the following guidance as to the preparation of the implementation documents:
>
> 1. The registrars' Model Dispute Resolution Policy should be used as a starting point;
>
> 2. The President or his delegate should convene a small drafting committee including persons selected by him to express views and consider the interests of the registrar, non-commercial, individual, intellectual property, and business interests;
>
> 3. In addition to the factors mentioned in paragraph 171(2) of the WIPO report, the following should be considered in determining whether a domain name was registered in bad faith:
>
> (a) Whether the domain name holder is making a legitimate noncommercial or fair use of the mark, without intent to misleadingly divert consumers for commercial gain or to tarnish the mark
>
> (b) Whether the domain name holder (including individuals, businesses, and other organizations) is commonly known by the domain name, even if the holder has acquired no trademark or service mark rights; and
>
> (c) Whether, in seeking payment for transfer of the domain name, the domain name holder has limited its request for payment to its out-of-pocket costs.
>
> 4. There should be a general parity between the appeal rights of complainants and domain name holders.
>
> 5. The dispute policy should seek to define and minimize reverse domain name hijacking.

138. *See* ICANN, *Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy* § 2.4, *available at* http://www.icann.org/udrp/udrp-second-staff-report-24oct99.htm (Oct. 24, 1999) (on file with the University of Illinois Law Review).

139. *Id.* § 1.6. For a detailed discussion of the UDRP's genesis and content, see A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy"—Causes and (Partial) Cures*, 67 BROOK. L. REV. 605 (2002) [hereinafter Froomkin, *Partial Cures*].

II. ANTITRUST IMMUNITY FOR STATE ACTION

A. The State Action Doctrine

Government agencies and those they authorize to act are immune from antitrust scrutiny. The principal source of such immunity is the "state action doctrine," which strictly speaking protects only actions by states and those they deputize, perhaps including municipal and county governments.[140] However, there are parallel immunity doctrines protecting both the United States government and foreign sovereigns.[141]

The purpose behind the state action doctrine is the subject of some dispute.[142] It is clear that the Court views government action as different in some fundamental respect from private action, though whether the source of that difference lies in the constitutional allocation of responsibilities to the states or in the antitrust laws themselves is unsettled. Regardless, the Court made it clear in *Parker v. Brown* that a state could immunize even naked private cartels from antitrust scrutiny if it were to require such anticompetitive conduct as a matter of state policy.[143] Similarly, Congress is free to exempt particular industries or kinds of conduct from the antitrust laws, so long as it does so expressly.[144] Indeed, because Congress is not subject to the dictates of the Supremacy Clause, it is free to repeal the antitrust laws themselves in whole or in part,[145] though the Court has proved reluctant to infer such a repeal in the absence of clear

140. *See* Parker v. Brown, 317 U.S. 341, 350–51 (1943); 1 PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW ¶ 221b (2d ed. 2000). The rules under which local governments are exempt under the state action doctrine are complex and irrelevant here. For a discussion, see *Community Communications Co. v. City of Boulder*, 455 U.S. 40, 50–51 (1982); *City of Lafayette v. La. Power & Light*, 435 U.S. 389, 412–13 (1978); and 1 AREEDA & HOVENKAMP, *supra*, ¶ 223.

141. *See* Foreign Sovereign Immunities Act, 28 U.S.C §§ 1330, 1602–1611 (2002); 1A AREEDA & HOVENKAMP, *supra* note 140, ¶ 252 (federal sovereign immunity); 1A *id.* ¶ 274d (foreign sovereign immunity).

142. There has been a great deal of academic literature devoted to this topic. While there are many different theories, the literature might reasonably be divided into those who believe that government officials can be expected to act altruistically, and therefore do not need or deserve antitrust oversight; and those who believe government officials are subject to capture or to the dictates of public choice theory, and therefore might be expected to act anticompetitively. In the former camp, see Einer Elhauge, *Making Sense of Antitrust Petitioning Immunity*, 80 CAL. L. REV. 1177, 1203–04 (1992); Einer Richard Elhauge, *The Scope of Antitrust Process*, 104 HARV. L. REV. 667, 687 (1991); and Steven Semeraro, *Demystifying Antitrust State Action Doctrine*, 24 HARV. J. L. & PUB. POL'Y 203, 218 (2000). In the latter, see Robert P. Inman & Daniel L. Rubinfeld, *Making Sense of the Antitrust State Action Doctrine: Balancing Political Participation and Economic Efficiency in Regulatory Federalism*, 75 TEX. L. REV. 1203, 1232–49 (1997); McGowan & Lemley, *supra* note 15, at 365; William H. Page, *Interest Groups, Antitrust, and State Regulation:* Parker v. Brown *in the Economic Theory of Legislation*, 1987 DUKE L.J. 618; and John S. Wiley, Jr., *A Capture Theory of Antitrust Federalism*, 99 HARV. L. REV. 713, 731 (1986).

143. *See Parker*, 317 U.S. at 341 (holding that California raisin growers' cartel that destroyed seventy percent of its crop every year to "stabilize" prices was immune from antitrust scrutiny because California law authorized the cartel).

144. *See, e.g.*, 1 AREEDA & HOVENKAMP, *supra* note 140, ¶ 219 (exemption for insurance); 1A *id.* ¶¶ 255–257 (labor exemption); 1A *id.* ¶¶ 249–251 (miscellaneous other exemptions).

145. *See* 1A *id.* ¶ 242d (federal immunity "quite similar" to state immunity, but federal immunity is always subject to the will of Congress, which can write immunity as broadly as it wishes).

evidence.[146] Importantly, though, only Congress, and not federal agencies, is entitled to waive or repeal the antitrust laws.

The paradigm case of antitrust immunity is where the government itself acts directly to restrain competition, for example by passing a law setting minimum prices or forbidding new entry into a market. Governments are themselves immune from antitrust liability in such cases, even though the restraint on competition may be quite egregious. In *City of Columbia v. Omni Outdoor Advertising, Inc.*,[147] for example, the Court immunized a city council from antitrust liability for banning new billboards, even though there was good evidence in the case that the mayor and other council members were good friends of the existing local billboard monopolist and acted at its behest.[148]

A closer question is presented when the defendant is a private actor who claims to be acting in accordance with state policy. In both federal and state immunity cases, the question of whether a private party shares a state's immunity depends on two facts: whether the government has *clearly articulated* its intent that the private party act anticompetitively (or at least without antitrust constraint), and whether the state has *actively supervised* the subsequent conduct of the private party.[149] Only if private action is both subject to a clearly articulated government policy and actively supervised by the government will it be entitled to antitrust immunity.

Some examples may help illuminate the scope of antitrust immunity for private actors. For example, in *California Retail*, California had enacted a statute that protected wine dealers by authorizing them to engage in "resale price maintenance"—the practice of preventing discounting by requiring that retailers sell at no less than a certain price. Minimum resale price maintenance is illegal per se under the federal antitrust laws,[150] and the question is whether wine dealers who engaged in such a scheme were immunized by the state statute from federal antitrust liability. In this case, the legislature was quite clear in articulating its policy.[151] The Court nonetheless rejected antitrust immunity because it found that the State had not actively supervised the wine dealers, but had merely delegated authority over price to them:

146. *See, e.g.*, Nat'l Gerimedical Hosp. & Gerontology Ctr. v. Blue Cross, 452 U.S. 378 (1981).

147. 499 U.S. 365 (1991).

148. *Id.* at 367. For a discussion of the case's facts, see McGowan & Lemley, *supra* note 15, at 312–14.

149. *See, e.g.*, FTC v. Ticor Title Ins. Co., 504 U.S. 621, 631 (1992); Cal. Retail Liquor Dealers Ass'n v. Midcal Aluminum, Inc., 445 U.S. 97, 105 (1980).

150. *See*, *e.g.*, 324 Liquor Corp. v. Duffy, 479 U.S. 335, 341–43 (1987); *Cal. Retail*, 445 U.S. at 102–03; United States v. Parke, Davis & Co., 362 U.S. 29, 47 (1960); Dr. Miles Med. Co. v. John D. Park & Sons Co., 220 U.S. 373, 407 (1911). Maximum resale price maintenance was once illegal per se, but no longer is. *See* State Oil Co. v. Khan, 522 U.S. 3, 22 (1997).

151. Indeed, the Court noted that "the legislative policy is forthrightly stated and clear in its purpose to permit resale price maintenance." *Cal. Retail*, 445 U.S. at 105.

> The state simply authorizes price setting and enforces the prices established by private parties. The State neither establishes prices nor reviews the reasonableness of the price schedules. . . . The national policy in favor of competition cannot be thwarted by casting such a gauzy cloak of state involvement over what is essentially a private price-fixing arrangement.[152]

Thus, the Court made it clear that government cannot simply abdicate its role to set and enforce policy to a private actor. To similar effect is *FTC v. Ticor Title Insurance Co*.[153] In that case, the Federal Trade Commission alleged that six title insurance companies had conspired to fix prices. The companies defended on the grounds that they belonged to "rating bureaus"—private entities organized by the companies themselves to set uniform rates for their members—that were themselves licensed by the states and authorized to set rates, subject only to a veto by the state regulators. If the State did not object to the rate within thirty days, it took effect.[154] The Court held this scheme illegal as well. It asked whether "the State has played a substantial role in determining the specifics of the economic policy."[155] Only where "the details of the rates or prices have been established as a product of deliberate state intervention, not simply an agreement among private parties," will the Court consider the State to have actively supervised the private restraint.[156]

The rationale of these cases is clear: "Absent such a program of supervision, there is no realistic assurance that a private party's anticompetitive conduct promotes state policy, rather than merely the private party's individual interests."[157] To justify antitrust immunity, the government must have not only the right and ability to overrule private decisions, but must actually exercise its power to review those decisions.[158] And despite the Court's early deference to a price-fixing scheme in *Parker v. Brown*, the clear articulation and active supervision requirements of late have proven difficult hurdles to clear.

152. *Id.* at 105–06.

153. 504 U.S. 621 (1992).

154. *Id.* at 629.

155. *Id.* at 635.

156. *Id*. at 634–35. The same result obtains even in the absence of pricing decisions, where the state has delegated authority over a marketplace to a private actor. *See* Patrick v. Burget, 486 U.S. 94, 102–03 (1988) (holding peer review by Board of Medical Examiners not immune as state action, despite state authorization, because the state did not actively supervise the Board). For an argument that constitutional concerns about improper delegation of government authority motivate the Court's rules in this area, see McGowan & Lemley, *supra* note 15, at 343–56.

157. *Patrick*, 486 U.S. at 101.

158. *Id.* at 100–01; *Ticor Title*, 504 U.S. at 638; *see also* Pinhas v. Summit Health, Ltd., 894 F.2d 1024, 1030 (9th Cir. 1989), *aff'd on other grounds*, 500 U.S. 322 (1991); Shahawy v. Harrison, 875 F.2d 1529, 1534–36 (11th Cir. 1989) (both finding that deferential state review of a medical board's decisions for procedural error or arbitrary or capricious action was inadequate to clothe the board with antitrust immunity). Federal law has since modified this rule in the medical context. *See* Health Care Quality Improvement Act of 1986, 42 U.S.C. §§ 11101–11111 (2000).

B. Antitrust Immunity for Network Solutions

Despite the rather strict set of requirements for antitrust immunity articulated in the previous section, ICANN's predecessor, NSI, fared extremely well in antitrust litigation based on its conduct before ICANN was formed. Several reported cases have considered antitrust claims against NSI based on its control of the DNS and its trademark dispute policies. None have found liability. District courts generally rejected antitrust liability on the grounds that NSI was acting under the authority of the federal government and was immune from suit. The appellate courts were more cautious in granting such immunity, however. In this section, we discuss those cases, as well as two sets of related decisions, before turning in the next section to consider their implications for ICANN.

Four district courts have considered whether NSI was immune from suit because it acted at the behest of the government in setting domain name policy. All four courts concluded that NSI was immune from antitrust scrutiny,[159] in each case applying a related doctrine known as "federal instrumentality" immunity.[160] The immunity described by these cases sweeps much more broadly than the state action antitrust immunity described in the previous section. Indeed, in *PG Media* and *Thomas*, the district courts expressly distinguished the state action cases, holding that federal immunity was broader and did not require proof of anything other than authorization pursuant to a government cooperative agreement.[161]

Appellate courts have been much more restrictive in their reading of NSI's immunity, however. In both *Thomas* and *Watts*, the circuit courts refused to rely on immunity principles at all, instead affirming the district court decision because of another defect in the plaintiffs' antitrust cases.[162] In *Thomas*, the D.C. Circuit found the question of NSI's immunity "not clearly settled."[163] It held that the United States government

159. *See* Beverly v. Network Solutions, Inc., No. C-98-0337-VRW, 1998 WL 320829, at *4 (N.D. Cal. June 12, 1998) (NSI immune because it is a private party "acting in compliance with a clearly articulated government program;" no mention of active supervision requirement); Thomas v. Network Solutions, Inc., 2 F. Supp. 2d 22 (D.D.C. 1998), *aff'd on other grounds*, 176 F.3d 500 (D.C. Cir. 1999); Watts v. Network Solutions, Inc., No. IP 98-1529-C, 1999 WL 778589, at *3 (S.D. Ind. May 7, 1999), *aff'd on other grounds*, 202 F.3d 276 (7th Cir. 1999) (unpublished table decision); PGMedia, Inc. v. Network Solutions, Inc., 51 F. Supp. 2d 389 (S.D.N.Y. 1999), *aff'd sub nom.* Name.space, Inc. v. Network Solutions, Inc., 202 F.3d 573 (2d Cir. 2000).

160. "Federal instrumentality" immunity protects agents acting on behalf of the federal government from liability for conduct ordered by the government. Federal "instrumentalities" are traditionally units or subdivisions of the government itself, rather than private actors. *See, e.g.*, Sakamoto v. Duty Free Shoppers Ltd., 764 F.2d 1285 (9th Cir. 1985) (Guam is a federal instrumentality immune from the antitrust laws); Champaign-Urbana News Agency, Inc. v. J.L. Cummins News Co., 632 F.2d 680 (7th Cir. 1980) (U.S. armed forces are federal instrumentalities immune from the antitrust laws).

161. *See Thomas*, 2 F. Supp. 2d at 38.

162. *See Thomas*, 176 F.3d at 509; *Watts*, 202 F.3d at 276.

163. *Thomas*, 176 F.3d at 508.

was clearly immune from suit under the antitrust laws.[164] In contrast, the court noted that "[i]t is not obvious to us . . . that a private contractor automatically shares the federal agency's immunity simply because the contractor's allegedly anticompetitive conduct occurred . . . 'pursuant' to a government contract. A contractor might be free to perform the contract in any number of ways, only one of which is anticompetitive."[165] The court did not decide the issue, choosing instead to address the deficiencies it perceived in the merits of the plaintiffs' antitrust claim.[166] The Seventh Circuit did the same thing in *Watts*. It noted that NSI's immunity was not automatic, as the district court had held, citing *Thomas*.[167] Like *Thomas*, the court chose to affirm on another antitrust ground, in that case standing, "rather than decide the complex issue of whether NSI enjoys antitrust immunity."[168] Because *Watts* is unpublished, however, its endorsement of the D.C. Circuit approach is of no precedential value.

The most detailed treatment of the issue is the Second Circuit's opinion in *Name.Space*.[169] In that case, the plaintiff had challenged NSI's refusal to create new gTLDs. NSI had initially decided to create new TLDs, but after consulting with the National Science Foundation, it was directed not to do so. NSI followed this directive and refused to create the new TLDs, whereupon the plaintiff sued it for violating the antitrust laws. The district court held that NSI was entirely immune from antitrust scrutiny under the federal instrumentality doctrine.[170]

On appeal, the Second Circuit refused to apply the federal instrumentality doctrine, reasoning that "reliance on such a broad rule of immunity might improperly insulate NSI and other private entities that are or will be involved in administering the DNS from liability for future anticompetitive conduct."[171] Rather, the court applied an immunity doctrine based largely on the state action doctrine. It had little trouble finding immunity in the case before it, however, because "the conduct being challenged by Name.Space in this appeal was compelled by the explicit terms of NSI's agreement with a government agency and by the govern-

164. *Id*. (citing United States v. Cooper Corp., 312 U.S. 600 (1941) (U.S. government not a "person" who can be sued under the Sherman Act); Sea-Land Serv., Inc. v. Alaska R.R., 659 F.2d 243 (D.C. Cir. 1981) (wholly owned and operated government corporation was immune from suit)).

165. *Thomas*, 176 F.3d at 508–09 (citing Otter Tail Power Co. v. United States, 410 U.S. 366 (1973)). In *Otter Tail*, the Court seemed to reject the idea that government contracts could confer antitrust immunity, noting that "government contracting officers do not have the power to grant immunity from the Sherman Act." 410 U.S. at 378–79. But the Court went on to suggest that some contracting parties may in fact be immune by virtue of their relationship to the government, leaving the Court's holding on this point less than clear.

166. *Thomas*, 176 F.3d at 509 (holding that plaintiffs had not made out the elements of an "essential facilities" claim).

167. *Watts*, 202 F.3d at 276.

168. *Id.*

169. Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573 (2d Cir. 2000).

170. PGMedia, Inc. v. Network Solutions, Inc., 51 F. Supp. 2d 387, 407 (S.D.N.Y. 1999).

171. *Name.Space*, 202 F.3d at 581.

ment's policies."[172] To require NSI to fulfill its contract, yet permit it to be sued for doing what the government required it to do, would be unfair.[173]

These cases suggest that NSI's antitrust immunity for conduct related to the DNS is far from clearly settled. In fact, it is unlikely that NSI will receive absolute immunity. Rather, immunity will be determined on the basis of traditional principles drawn from the state action cases: whether the government clearly articulated a policy that required interference with competition, and whether the government actively supervised private decision making in accordance with that policy.

Two other sets of cases deserve brief mention here. First, two domain name antitrust decisions have rejected the plaintiffs' claims for failure to define a proper economic market.[174] While these cases are not directly relevant to antitrust immunity, they do remind us of the important point that immunity is not all there is to antitrust law. Even if NSI is not immune from antitrust scrutiny, an antitrust plaintiff will have to prove all the elements of a § 2 claim to prevail. We discuss potential antitrust claims in more detail in part III.

Second, two courts have considered whether NSI is a state actor in a different context: whether it must conform its conduct to the Constitution and, in particular, to the First Amendment. In both cases, the courts concluded that NSI was not a state actor for First Amendment purposes.[175] The courts emphasized the facts that registering domain names is not a traditional governmental function,[176] that the government did not impose restrictive regulatory oversight on NSI, and that the "nexus" between the government and NSI was not sufficiently close to find that the two were in a symbiotic relationship.[177] The standards for state action in the First Amendment context are different than in the antitrust context,[178] and the courts' conclusions are certainly contestable on their mer-

172. *Id.* at 582.

173. *Id*. at 583 (quoting Alpha Lyracom Space Communications, Inc. v. Communications Satellite Corp., 946 F.2d 168, 174 (2d Cir. 1991) ("Congress could not have intended to require [a private entity] to [act] subject to [federal governmental] directives and, at the same time, have intended that [it] proceed at its own antitrust peril in carrying out that official role.") (alterations in original) (citations omitted)).

174. Smith v. Network Solutions, Inc., 135 F. Supp. 2d 1159, 1168–70 (N.D. Ala. 2001) (holding there is no relevant economic market for "expired domain names"); Weber v. Nat'l Football League, 112 F. Supp. 2d 667, 673–74 (N.D. Ohio 2000) (stating there is no relevant economic market for a subset of domain names that constitute NFL trademarks).

175. Island Online, Inc. v. Network Solutions, Inc., 119 F. Supp. 2d 289, 303–07 (E.D.N.Y. 2000); Nat'l A-1 Adver., Inc. v. Network Solutions, Inc., 121 F. Supp. 2d 156, 165–69 (D.N.H. 2000).

176. The courts disagreed on this point. *Compare National A-1 Advertising*, 121 F. Supp. 2d at 167 (finding that registration of domain names is a traditional governmental function), *with Island Online*, 119 F. Supp. 2d at 306 (holding the opposite). The D.C. Circuit weighed in on the latter side in *Thomas v. Network Solutions, Inc.*, 176 F.3d at 500, 511 (D.C. Cir. 1999).

177. *Island Online*, 119 F. Supp. 2d at 304–07; *National A-1 Advertising*, 121 F. Supp. 2d at 166–69.

178. For a discussion of the First Amendment standards, see, e.g., Paul Brest, *State Action and Liberal Theory: A Casenote on* Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296 (1982); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503 (1985).

its.[179] Still, it is interesting that in the constitutional context, courts have minimized the extent to which NSI acts at the government's behest. The facts they cite may turn out to be quite relevant to the antitrust immunity inquiry as well.

C. Antitrust Immunity for ICANN?

Given this legal background, and what we learned about ICANN's relationship to the government in part I, what are ICANN's prospects for antitrust immunity? As an initial matter, it seems safe to say that ICANN will not be able to rely on an absolute form of federal instrumentality immunity. Congress has not created an express exception to the antitrust laws for ICANN. Indeed, it has not spoken at all on the subject. So if ICANN is to be immune from antitrust suit, it must be because of its contracts with the DoC. But appellate courts so far have not endorsed the theory that any government contractor is entitled to absolute immunity. Instead, federal instrumentality immunity has been limited to units or divisions of the federal government. Rather, the most likely approach will be one akin to the state action doctrine: a case-by-case analysis of whether ICANN's actions were pursuant to a clearly articulated governmental policy to displace competition and were actively supervised by the government.

We are skeptical that all of ICANN's conduct can meet that test. ICANN does have an argument on the clearly articulated government policy prong, but the facts currently in the public record suggest that it would have a very hard time showing the necessary degree of active government supervision and involvement in its implementation of that policy.[180] Of course, it is always possible that ICANN would be able to demonstrate that the government has had a far greater behind-the-scenes involvement in ICANN's decisions than either the DoC or ICANN has admitted. At present, however, we take the parties at their word that since its formation, the DoC has given ICANN very great independence.

The White Paper can be used to argue both sides of the "clearly articulated government policy" test.[181] On the one hand, the White Paper itself considered and rejected the idea that 'NewCo,' as it then was, should be given antitrust immunity. Indeed, in the White Paper the government argued that "[a]pplicable antitrust law will provide accountability to and protection for the international Internet community. Legal challenges and lawsuits can be expected within the normal course of

179. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 113–25 (arguing that ICANN is a state actor for constitutional purposes). *See generally* Berman, *supra* note 6.

180. *Accord* Sims & Bauerly, *supra* note 6, at 84–90 (explaining in detail why ICANN should not be considered a state actor for constitutional purposes).

181. *See* Tamar Frankel, *The Managing Lawmaker in Cyberspace: A Power Model*, 27 BROOK. J. INT'L. L. 859, 863 (2002) ("[ICANN's] accountability to a 'higher authority,' such as the Department of Commerce, is unclear.").

business for any enterprise and the new corporation should anticipate this reality."[182] This seems if anything a fairly clearly articulated policy that there *not* be antitrust immunity.[183]

On the other hand, the White Paper also contained a number of policy directions for NewCo, instructions that ICANN has on the whole faithfully followed. For example, in the White Paper the DoC clearly articulated a view that the DNS needed an anticybersquatting policy, and stated that the policy, whatever it was, should be put into place by a new nonprofit corporation that took over administration of the DNS.[184] That said, the White Paper had relatively little to say about the details.[185] Whether this general, but emphatic, statement in a legally nonbinding "policy statement," and the Department's subsequent praise for the UDRP constitutes a sufficiently clear federal policy that there should be a UDRP certainly could be debated.[186] Any such debate would be en-

182. White Paper, *supra* note 31, at 31,747.

183. *But see* Lebron v. Nat'l R.R. Passenger Corp., 513 U.S. 374, 400 (1995) (holding that congressional statement that otherwise public corporation was private did not make it private for First Amendment purposes).

184. White Paper, *supra* note 31, at 31,747.

185. The White Paper stated:

> "[T]he U.S. Government recommends that the new corporation adopt policies whereby:
>
> 1) Domain registrants pay registration fees at the time of registration or renewal and agree to submit infringing domain names to the authority of a court of law in the jurisdiction in which the registry, registry database, registrar, or the "A" root servers are located.
>
> 2) Domain name registrants would agree, at the time of registration or renewal, that in cases involving cyberpiracy or cybersquatting (as opposed to conflicts between legitimate competing rights holders), they would submit to and be bound by alternative dispute resolution systems identified by the new corporation for the purpose of resolving those conflicts. Registries and Registrars should be required to abide by decisions of the ADR system.
>
> 3) Domain name registrants would agree, at the time of registration or renewal, to abide by processes adopted by the new corporation that exclude, either pro-actively or retroactively, certain famous trademarks from being used as domain names (in one or more TLDs) except by the designated trademark holder.
>
> 4) Nothing in the domain name registration agreement or in the operation of the new corporation should limit the rights that can be asserted by a domain name registrant or trademark owner under national laws.

Id. ICANN's ultimate plan substantially complied with 1 and 2, but not 3. It attempted to comply with 4, although how successful it was is hotly debated. *See* Froomkin, *Partial Cures*, *supra* note 139, at 623.

186. Indeed, several district court opinions come down on opposite sides of this question. In *Eurotech, Inc. v. Cosmos European Travels Aktiengesellschaft*, 189 F. Supp. 2d 385, 393 (E.D. Va. 2002), the court held that because the WIPO is a public body and the DoC participated in the creation of the UDRP, the UDRP is sufficiently public to entitle UDRP plaintiffs to the same *Noerr-Pennington* immunity granted to litigants in federal courts. Only a few weeks later, however, in *Bord v. Banco de Chile*, 205 F. Supp. 2d 521, 524 (E.D. Va. 2002), another judge on the same court held that the DoC's participation in the creation of the UDRP was too tenuous to allow a plaintiff standing to blame the DoC for the UDRP. Specifically, the *Bord* court concluded that "the Memorandum between DOC and ICANN does not bind ICANN in any way to commit to a dispute resolution policy, nor does it require ICANN to compel registrants to agree to a dispute resolution policy." *Id.; see also* Frogface, Inc. v. Network Solutions, Inc., No. C-00-3854-WHO, 2002 WL 202371, at *3 (N.D. Cal. Jan. 14, 2002) ("[T]here is no authority for the proposition that ICANN policies have the force of law."); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 247 (S.D.N.Y. 2000) (finding that the DoC delegation to ICANN was a general policy statement, not a regulatory scheme).

The *Eurotech* decision is problematic as both a legal and a policy matter. On the legal side, it seems clear that UDRP panelists are *not* government entities whom U.S. citizens are constitutionally entitled

riched by arguments that even if the DoC had a policy favoring some kind of uniform dispute policy, it lacked the statutory authority to make such a policy. The ultra vires argument rests on the assertion that the DoC has no specific statutory authority or obligation to control the DNS or the legacy root,[187] and the observation that the Administrative Dispute Resolution Act (ADRA) generally prohibits an agency from requiring arbitration to settle "the resolution of an issue in controversy that relates to an administrative program."[188] The problem here for ICANN is that if the DoC directly required the UDRP, it probably violated ADRA.[189] If it did not directly require the UDRP, it is hard to argue that the federal policy was sufficiently explicit to meet the "clear articulation" and "active supervision" tests. Similarly, it is evident that the DoC intended for one of ICANN's tasks to be the selection of new gTLDs, but other than defining general principles designed to guide ICANN, the DoC did not instruct it as to how to go about picking TLDs or registries.

Even if ICANN were able to prevail on the "clearly articulated" prong, on the facts publicly available, its chances of prevailing on the "active supervision" requirement look slim. Although the DoC may have set out specific tasks for ICANN to achieve, such as the prevention of cyberpiracy, both ICANN and the DoC have asserted that ICANN acts independently of U.S. government control. Indeed, ICANN seems to be a paradigmatic case of a contractor left "free to perform the contract in any number of ways."[190] There are no defined procedures by which the DoC reviews ICANN's work,[191] and even in the case of additions to the root, where the DoC retains final authority to alter or countermand

to petition. *Cf.* McGowan & Lemley, *supra* note 15, at 363–65 (arguing that *Noerr* immunity is a function of the First Amendment right to petition, and rejecting contrary interpretations). They are privately employed, and are not subject even to the dictates of the Federal Arbitration Act. *See, e.g.*, Parisi v. Netlearning, Inc., 139 F. Supp. 2d 745, 751–52 (E.D. Va. 2001). While the WIPO itself is an international organization, the WIPO does not itself act in domain name decisions. On the policy side, *Eurotech* appears to have created a rule that favors the WIPO over other UDRP dispute resolution providers, since only the WIPO is an international organization. Further, the checks that exist in the judicial context against misrepresentations—Rule 11 sanctions, a court's contempt power, the rules of evidence, and the presence of opposing counsel who can correct false statements—are notably absent from UDRP proceedings.

187. Such at least was the GAO's view. *See* GAO REPORT, *supra* note 61.

188. Administrative Dispute Resolution Act (ADRA), 5 U.S.C. §§ 571–583 (2000). An "issue in controversy" is defined as "an issue which is material to a decision concerning an administrative program of an agency, and with which there is disagreement" either "between an agency and persons who would be substantially affected by the decision" or "between persons who would be substantially affected by the decision." *Id.* § 571(8)(A)–(B); *see also* Froomkin, *Wrong Turn*, *supra* note 3, at 135–36.

189. There being no relevant case law, it remains possible for the DoC to argue that by using a contractor to execute its policy, it somehow took itself out of ADRA's reach.

190. One of us has argued that ICANN is in fact *too* free of government control, and that the DoC's grant of so much discretion to ICANN amounts to a violation of the nondelegation doctrine in *Carter v. Carter Coal, Co.*, 298 U.S. 238 (1936). *See* Froomkin, *Wrong Turn*, *supra* note 3.

191. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 107–13; Helfer & Dinwoodie, *supra* note 3, at 180–82 (arguing that ICANN is not subject to effective scrutiny). *But see supra* note 83 and accompanying text (noting GAO recommendation that the DoC monitor ICANN more closely).

ICANN's decisions,[192] the DoC has stated that it does not intend to exercise any substantive review.[193] The DoC *has* intervened in ICANN policy making on rare occasions, but these primarily concerned ICANN's relationship with NSI/VeriSign, another government contractor. In 1999, the DoC was intensively involved in brokering a deal between ICANN and NSI in which NSI agreed to recognize ICANN's authority over it in exchange for an extension of its monopoly on the .com, .net and .org registries and certain limits on ICANN's freedom to regulate it.[194] Another intensive intervention came when several influential legislators objected to ICANN's proposed revisions to the ICANN-NSI/VeriSign contract, a change that required DoC approval under the earlier set of agreements.[195] The DoC and the U.S. Department of Justice stepped in and altered the agreement to reflect antitrust concerns arising from VeriSign's retention of ownership in both the dominant registries and the dominant registrar.[196]

In contrast, other than the statements in the White Paper, there is little in the public record to suggest that the DoC instructed ICANN as either to the content of the UDRP or the ways in which ICANN should manage the selection of arbitration service providers. The main signs of continuing DoC involvement have been: (1) in July 1999, a DoC official told a House Subcommittee that the DoC had been consulting with ICANN before ICANN's major decisions, such as ICANN's proposal to charge a fee of one dollar per domain name;[197] (2) in the June 2000 MoU, the DoC promised to devote more than a quarter of a million dollars in staff time and expenses to monitoring and helping ICANN, which the DoC estimated would equal half-time dedication of four or five employees;[198] and (3) in July 2000, ICANN's board passed resolution of thanks to outgoing NTIA official Becky Burr mentioning her "enormous contributions."[199] Other than these, there is little sign that the government has

192. *See Cooperative Agreement*, *supra* note 41.

193. *See supra* note 68 and accompanying text.

194. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 89–91.

195. *See* A. Michael Froomkin, *US House Leaders Warn on VeriSign Deal*, ICANNWATCH (Mar. 30, 2001), *available at* http://www.icannwatch.org/article.php?sid=72 (on file with the University of Illinois Law Review); A. Michael Froomkin, *House Democrats Up the Ante on ICANN/VeriSign Deal*, ICANNWATCH (May 16, 2001), *available at* http://www.icannwatch.org/article.php?sid=154 (on file with the University of Illinois Law Review); Letter from Rep. John D. Dingell, Ranking Member, Comm. on Energy and Commerce, and Rep. Edward J. Markey, Ranking Member, Subcomm. on Telecommunications and the Internet, to Donald L. Evans, Secretary, Dep't Commerce (May 15, 2001), *available at* http://www.house.gov/commerce_democrats/press/107ltr53.htm (on file with the University of Illinois Law Review).

196. *See* Froomkin, *SPIN CYCLE*, *supra* note 74.

197. Letter from Andrew J. Pincus, to Rep. Tom Bliley, *supra* note 56, § B.3.

198. *Memorandum of Understanding*, *supra* note 50, app. B.

199. Along with her colleagues at the Department of Commerce, she played an essential facilitating role in not only the creation of ICANN, but also in its creation of contractual relationships with many of the important elements of the Internet community which have been and will be instrumental in its continued viability as an effective global, private sector, consensus creation body.

It would not be an overstatement to conclude that, without the enormous contributions of Becky Burr, ICANN would not be here today, or at a minimum would not have made the very

had a role in supervising the (controversial[200]) administration of the UDRP beyond mere general cheerleading,[201] although one presumes those DoC employees were doing something.

Similarly, there is nothing in the public record to suggest that the DoC took an active role in ICANN's selection of new gTLDs. The DoC's role appears to have been limited to giving ICANN authority to select new gTLDs in its initial contracts, and in its rubber-stamp approval of ICANN's choices, with little or nothing in between. The high water mark of the DoC's intervention appears to have been a recent letter from Secretary of Commerce Evans to ICANN—long after the first round selection process was over—to urge it to approve the next round of domains more quickly.[202] The facts that Secretary Evans felt a need to write to ICANN, rather than just instruct it, and that the letter appears to have had no effect whatsoever,[203] both argue strongly that ICANN's selection of new gTLDs is not subject to close supervision by the DoC.

ICANN's resistance to alternate roots follows the same pattern. Again, the policy arguably has its origins in the White Paper, which stated that "[t]he introduction of a new management system should not disrupt current operations or create competing root Systems."[204] Similar language did not, however, get included in the ICANN-DoC MoU.[205] In

significant progress that is reflected at this meeting. She could not have done it alone, but we could not have done what we have done without her tireless devotion to the objective of a viable and effective ICANN.

ICANN, *Preliminary Report: Meeting of the ICANN Board in Yokohama*, Resolution 00.69, *available at* http://www.icann.org/minutes/prelim-report-16jul00.htm (July 16, 2000) (on file with the University of Illinois Law Review).

200. *See*, *e.g.*, Froomkin, *Partial Cures*, *supra* note 139; Michael Geist, *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, 27 BROOK. J. INT'L L. 903 (2002); Milton Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, CONVERGENCE CENTER, *available at* http://dcc.syr.edu/roughjustice.htm (last visited Sept. 2, 2002) (on file with the University of Illinois Law Review); Kenneth L. Port, *Trademark Monopolies in the Blue Nowhere*, 28 WM. MITCHELL L. REV. 1091 (2002); Elizabeth G. Thornburg, *Going Private: Technology, Due Process, and Internet Dispute Resolution*, 34 U.C. DAVIS L. REV. 151 (2000).

201. A NTIA report praised the UDRP as "an efficient, inexpensive procedure for the resolution of disputes." 2000 NAT'L TELECOMM. & INFO. ADMIN. ANN. REP., *available at* http://www.ntia.doc.gov/ntiahome/annualrpt/2001/2000annrpt.htm (last visited Aug. 22, 2002) (on file with the University of Illinois Law Review).

202. *See* David McGuire, *Commerce Department Urges ICANN to Add More New Domains*, NEWSBYTES (May 25, 2001), *available at* http://www.info-sec.com/commerce/01/commerce_05250la_j.shtm (on file with the University of Illinois Law Review).

203. As noted above, ICANN has barely even begun a process for deciding on a process for evaluating additional TLDs. *See supra* notes 106–23 and accompanying text.

204. White Paper, *supra* note 31, at 31,749.

205. *Compare* White Paper, *supra* note 31, at 31,743:

> The U.S. Government should end its role in the Internet number and name address system in a manner that ensures the stability of the Internet. The introduction of a new management system should not disrupt current operations or create competing root systems. During the transition and thereafter, the stability of the Internet should be the first priority of any DNS management system. Security and reliability of the DNS are important aspects of stability, and as a new DNS management system is introduced, a comprehensive security strategy should be developed.

with Memorandum of Understanding, *supra* note 50, § C.1:

> This Agreement promotes the stability of the Internet and allows the Parties to plan for a deliberate move from the existing structure to a private-sector structure without disruption to the

particular, there is no evidence that ICANN's refusal to even consider applications from firms that enabled alternate roots was required by the government.[206] This is particularly important because ICANN's revenue base depends on its being in charge of the only root of any importance. ICANN thus stands to gain from keeping its monopoly, and the government effectively delegated market control to a private party with an interest in the outcome. While the government is free to do this, the delegate is entitled to antitrust immunity only if the government actively supervises its conduct. Where private conduct directly restricts competition, that supervision must include direct control over the price or output setting, not merely a generalized delegation of authority.[207] This does not appear to be the case with ICANN.

It is true that NSI has so far avoided antitrust liability for its actions in running the DNS during a prior era. But ICANN may not fare so well. Most of the cases against NSI were in fact ultimately resolved on the antitrust merits, not on grounds of antitrust immunity.[208] The one case ultimately finding immunity relied on the fact that NSI was specifically directed to engage in the challenged practice by the government.[209] ICANN may be able to point to similar government mandates in a few cases, but surely cannot justify all its policies in this way. As one court put it, "the government's role in the Internet is deliberately waning. By design, the private sector is assuming an ever-increasing role in determining relevant policies and protocols, and domain name registration is now a competitive endeavor . . . ."[210] ICANN was intended to get the U.S. government out of the business of running the DNS. While the government certainly has not succeeded completely in disentangling itself from the DNS, it gives less policy direction and less direct oversight to ICANN than it did to NSI in the mid-1990s.[211] With ICANN's increased authority comes responsibility under the antitrust laws. ICANN's actions may or

functioning of the DNS. The Agreement calls for the design, development, and testing of a new management system that will not harm current functional operations.

206. For a discussion of alternate roots and their competitive implications, see *infra* notes 256–63 and accompanying text.

207. *See, e.g.*, A.D. Bedell Wholesale Co. v. Philip Morris, Inc., 263 F.3d 239, 264 (3d Cir. 2001) (holding that state action doctrine does not provide immunity from an allegation that a state government-tobacco settlement facilitates a cartel; while the government clearly articulated its policy of restricting production of cigarettes, the states "lack oversight or authority over the tobacco manufacturers' price and production levels. These decisions are left entirely to the state actors." This constituted inadequate state supervision).

208. *See supra* notes 159–68 and accompanying text.

209. Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573, 582 (2d Cir. 2000).

210. Nat'l A-1 Adver., Inc. v. Network Solutions, Inc., 121 F. Supp. 2d 156, 166 (D.N.H. 2000); *see also* Zittrain, *supra* note 6, at 1092 (describing ICANN as taking a "middle path" between public and private status).

211. *But see* Froomkin, *Form and Substance*, *supra* note 60, at 116 (arguing that ICANN behaves more like a government actor, albeit with less supervision from the DoC, than NSI did).

may not violate the antitrust laws; we turn to that subject in the next part. But it is not entitled to ignore those laws altogether.[212]

III. IS ICANN VIOLATING THE ANTITRUST LAWS?

Assuming that ICANN is not immune from antitrust liability,[213] the next step is to consider the merits of antitrust claims likely to be brought against it.[214] In this part, we consider the merits of four likely antitrust challenges: a claim that the DNS and/or the TLDs are essential facilities to which ICANN must open access on reasonable and nondiscriminatory terms; a claim that ICANN's refusal to accredit registrars who are affiliated with alternative or competitive roots is an act of monopolization; a claim that ICANN's insistence on registrars' adherence to uniform mandatory dispute resolution policies is an illegal cartel; and a claim that VeriSign's "Waiting List Service," as approved by ICANN, is an exclusive dealing arrangement with anticompetitive consequences.

A. Principles of Antitrust Law

Antitrust law treats unilateral conduct under the law of monopolization. The governing statute is § 2 of the Sherman Act, which sweeps broadly to condemn "every person who shall monopolize, or attempt to monopolize," a relevant market.[215] The concept of monopolization embodies two crucial principles. First, to be liable under § 2 of the Sherman Act, a defendant must be a monopolist, or at least be likely to become a monopolist.[216] Antitrust law does not generally scrutinize the unilateral conduct of individuals or companies; those who hold a monopoly position in a market are an exception to this general rule. Second, the mere possession or even acquisition of a monopoly is not illegal.[217] Rather, the offense of monopolization requires not just a monopoly, but some sort of anticompetitive conduct designed to acquire or maintain that monopoly.

212. The decreasing role of the government also makes it likely that VeriSign, NSI's successor company, will no longer enjoy immunity for its conduct. Indeed, the May 2001 revision of the contract between ICANN and VeriSign makes it clear that the DoC does not intend to immunize VeriSign from antitrust scrutiny. *See, e.g.*, *Department of Commerce Approves ICANN Registry Agreements with VeriSign Inc.*, 6 ELEC. COMM. & L. REP. 567 (2001).

213. As we noted in Part II, there is some question as to ICANN's immunity. But for the remainder of this part and the next, we will assume that ICANN is not categorically immune from antitrust liability.

214. While we are aware of no reported antitrust decisions involving ICANN to date, the proliferation of claims against NSI—including some still being filed after ICANN took over suggest that such cases are coming. *See, e.g.*, Chrysalis Vineyards v. U.S. Department of Commerce, No. 00-1330-A (E.D. Va. filed Sept. 7, 2000) (closed as of May 2002).

215. 15 U.S.C. § 2 (2000).

216. *See id.*

217. *See, e.g.*, United States v. United Shoe Mach. Corp., 110 F. Supp. 295, 297 (D. Mass. 1953) (acquisition of monopoly power by "superior skill, superior products, natural advantages, economic or technological efficiency," and other means is not illegal).

Thus, in *United States v. Grinnell Corp.*,[218] the Court defined monopolization under § 2 as follows:

> (1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.[219]

These limitations are designed to balance two competing policy interests. On the one hand, the antitrust law reflects an economic judgment that competition is desirable and monopolies are undesirable. Competition is good for a variety of reasons. Basic economics teaches that firms in competition will produce more and price lower than monopolists. Monopolists not only take money away from consumers by raising prices, but they impose a "deadweight loss" on society by reducing their output below the level which consumers would be willing to purchase at a competitive price. As a result, some transactions that would make economic sense (because consumers value the product at more than it would cost to produce it) do not occur.[220] Monopoly has other problems as well. It inherently reduces consumer choice, and monopolists have fewer incentives to innovate than do competitive firms.

At the same time, the law does not forbid all monopolies. Some monopolies result from natural economic conditions that permit only one firm to operate efficiently in a given market. Such "natural monopolies" include the physical cables for the so-called last mile of local distribution of electric power and telephone service. Other monopolies result from vigorous competition on the merits—precisely the sort of behavior the antitrust law is designed to encourage. Still other monopolies result from a firm's innovation, either because the innovation makes the firm more efficient or because legally granted intellectual property rights give the firm a certain measure of control over a market.[221] If the law forbade every monopoly, it would discourage innovation and competition by causing large companies to worry too much about questionable behavior.[222] The § 2 cases attempt to strike a balance by prohibiting only monopolies acquired or maintained by anticompetitive means.

Section 1 of the Sherman Act forbids agreements in restraint of trade.[223] Courts have identified two basic types of agreements that may

218. 384 U.S. 563 (1966).

219. *Id*. at 570–71.

220. For a detailed discussion of the economic intuition here, see 2A AREEDA & HOVENKAMP, *supra* note 140, ¶¶ 402–415.

221. We do not mean to suggest that intellectual property rights normally confer market power; far from it. Normally they do not. *See* 1 HERBERT HOVENKAMP ET AL., IP AND ANTITRUST § 4.2 (2002). But intellectual property rights do sometimes provide competitive advantages to their owners. When they do, it would undermine the intellectual property laws to make it illegal to take advantage of those rights.

222. This is particularly true since, as we shall see, the remedies for an antitrust violation can include treble damages, structural relief breaking up a company, and even criminal penalties.

223. 15 U.S.C. § 1 (2000).

be in restraint of trade—agreements among competitors (called "horizontal restraints") and agreements between buyers and sellers (called "vertical restraints").[224] Vertical restraints are generally less threatening to competition than horizontal restraints. With the exception of vertical price fixing, they are generally judged under the "Rule of Reason." Under the Rule of Reason, courts balance the anticompetitive harms of a restraint against its procompetitive benefits.[225] Only those restraints which produce harms significantly in excess of benefits to competition are deemed unreasonable.

Horizontal restraints are more troubling because they may allow the participants to create a cartel that can then behave anticompetitively, much as a monopolist would. At first, most agreements between competitors were deemed illegal "per se," without any necessity for a weighing of harms and benefits to competition.[226] Today, the Supreme Court has retreated from that position, recognizing that certain agreements among competitors may be efficient and procompetitive.[227] Most horizontal restraints are now judged under the Rule of Reason. Only certain forms of "naked" agreements to fix prices or divide territories remain illegal per se.[228] Nonetheless, it is fair to say that antitrust treats agreements among competitors more harshly than it does unilateral conduct.

While the antitrust laws apply only to acts "in commerce," it is clear that ICANN's nonprofit status will not protect it. Antitrust law reaches nonprofit concerns so long as they engage in activities that affect commerce.[229] ICANN clearly does so. Thus, we turn in the following sections to the substantive antitrust issues that are likely to be raised by ICANN's conduct to date.

B. DNS as an Essential Facility

One sort of monopolization case departs from the general rules articulated above because it does not involve "conduct" at all in the affirmative sense. Courts sometimes hold that a monopolist has a duty to deal with competitors, or at least to continue a relationship once it has

224. Actually, the term "vertical restraints" refers to a whole class of transactions between companies in a vertical relationship in the chain of distribution, including dealers, franchisors, distributors, resellers, etc. *See generally* HERBERT HOVENKAMP, FEDERAL ANTITRUST POLICY §§ 11.1 n.1, 11.2 (2d ed. 1999) [hereinafter HOVENKAMP, ANTITRUST POLICY].

225. *See, e.g.*, Chi. Bd. of Trade v. United States, 246 U.S. 231, 238 (1918).

226. *See, e.g.*, United States v. Socony-Vacuum Oil Co., 310 U.S. 150, 223 (1940).

227. *See, e.g.*, Broad. Music, Inc. v. CBS, 441 U.S. 1, 8–9 (1979).

228. *Id.* at 13, 20.

229. *See, e.g.*, NCAA v. Bd. of Regents, 468 U.S. 85, 100 n.22 (1984); 1A AREEDA & HOVENKAMP, *supra* note 140, ¶ 261; TOMAS J. PHILIPSON & RICHARD A. POSNER, ANTITRUST AND THE NOT-FOR-PROFIT SECTOR (Nat'l Bureau of Econ. Research, Working Paper No. 8126, 2001), *available at* http://www.nber.org/papers/w8126 (on file with the University of Illinois Law Review).

begun.[230] Under this doctrine, the monopoly owner of an "essential facility" for competition may be forced to give access to that facility to competitors on reasonable and nondiscriminatory terms.[231] The essential facilities doctrine is unique in that a monopolist's status as the owner of the facility and a competitor in the market that relies on the facility, rather than any affirmative conduct, determines liability.[232]

The essential facilities doctrine grew out of a number of cases in which one company (or a group of them) had exclusive control over some facility and used that control to gain an advantage over competitors in an adjacent or downstream market. Most of the canonical cases have this basic structure. Thus, in *Terminal Railroad*, a group of railroads jointly owned a key bridge over the Mississippi River and accompanying rail yard, and refused to give competing railroads use of the facilities.[233] In *Otter Tail*, the public utility that owned all the transmission lines into a municipality refused to allow the municipality to "wheel" power over those lines from outside plants, because the utility itself wanted to provide power to the municipality.[234] And in *MCI v. AT&T*, the prebreakup Bell System refused to permit MCI to connect its long distance calls to the Bell System's local phone exchanges.[235] In each of these cases, the defendant owned a facility that could not plausibly be duplicated, and also participated in a competitive downstream market that required access to the facility. By denying access to the facility, the defendant either eliminated its downstream competitors or imposed significant costs on them.[236]

In *MCI*, the 7th Circuit set out a four-part test for an essential facilities claim:

> (1) control of the essential facility by a monopolist; (2) a competitor's inability practically or reasonably to duplicate the essential fa-

230. On the latter concept, see *Aspen Skiing Co. v. Aspen Highlands Skiing Corp*., 472 U.S. 585, 604–05, 611 (1985) (finding a refusal to continue dealing by a monopolist illegal in the absence of a legitimate business justification).

231. For a detailed discussion of the essential facilities doctrine, see 3A AREEDA & HOVENKAMP, *supra* note 140, ¶¶ 770–774.

232. The monopolist in an essential facilities case may be thought to have "acted" in some sense, by refusing to deal or to continue dealing with a competitor. But generally speaking a unilateral refusal to deal is not the sort of anticompetitive conduct with which the antitrust law is concerned.

233. United States v. Terminal R.R. Ass'n, 224 U.S. 383, 391, 394 (1912).

234. Otter Tail Power Co. v. United States, 410 U.S. 366, 368–69 (1973).

235. MCI Communications Corp. v. AT&T, 708 F.2d 1081, 1097 (7th Cir. 1983).

236. A very different sort of essential facility-type claim is envisioned by those few cases that impose a duty to continue dealing. For example, in *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585 (1985), the Court held that a ski company that owned three of the four mountains in a local area was obligated to continue offering a multi-area skiing pass with its sole competitor in that local area. While the Court did not discuss the case in essential facilities terms, there is no other antitrust concept that readily fits these circumstances. By avoiding the use of essential facilities language, however, the Court short-circuited inquiry into how important the multi-area pass actually was to competition.

> cility; (3) the denial of the use of the facility to a competitor; and (4) the feasibility of providing the facility.[237]

If such a claim is made out, the defendant will be obligated to provide access to the facility on reasonable and nondiscriminatory terms.[238]

Under this test, the defendant must be a monopolist, and the facility must be "essential" in the sense that the competitor needs access to it compete. An essential facility will therefore normally be an input into the competitive market—some component that must be used in providing the competitive product or service. The need must be substantial; inconvenience or cost increase resulting from unavailability should not suffice.[239] The court's test also offers a defense of legitimate business justification, by permitting the defendant to show that it was not feasible to provide access to the facility.[240] The "reasonable and nondiscriminatory terms" language also limits the defendant's obligation in circumstances where particular plaintiffs cannot afford to pay, are not willing to pay a reasonable price, or the like.[241]

While the *MCI* court does not discuss it directly, it seems important to add that withholding an essential facility is illegal only if it has the effect of foreclosing competition in the downstream market, and therefore of helping the defendant to acquire or maintain a monopoly in that market. Thus, the owner of the facility in question must be vertically integrated into the market in which competition is being foreclosed. *Otter Tail* and *MCI* both had such a characteristic. In the absence of such a market effect, condemning a truly unilateral refusal to deal could open the door to all sorts of claims in which competition is not really at stake.

The essential facilities doctrine has been heavily criticized. Many prominent antitrust scholars have argued that the doctrine should be abolished outright.[242] Others who favor the continued existence of the doctrine nonetheless concede that it is properly applied only in rare cases.[243]

237. *MCI Communications*, 708 F.2d at 1132–33.

238. *Id.* at 1132.

239. *See* Alaska Airlines, Inc. v. United Airlines, Inc., 948 F.2d 536, 544–45 (9th Cir. 1991) (airline computer reservation system was not an essential facility because airlines could compete without it, albeit at higher cost).

240. *MCI Communications*, 708 F.2d at 1132–33.

241. Whether this defense would extend to other sorts of business justifications for refusing to deal is unclear.

242. *See, e.g.*, HOVENKAMP, ANTITRUST POLICY, *supra* note 224, § 7.7 ("The so-called essential facility doctrine is one of the most troublesome, incoherent and unmanageable of bases for Sherman § 2 liability. The antitrust world would almost certainly be a better place if it were jettisoned . . . ."); David McGowan, *Regulating Competition in the Information Age: Computer Software as an Essential Facility Under the Sherman Act*, 18 HASTINGS COMM. & ENT. L.J. 771, 850 (1996) ("[T]he essential facilities doctrine has no place in the legal regime being crafted to regulate software.").

243. *See* Philip Areeda, *Essential Facilities: An Epithet in Need of Limiting Principles*, 58 ANTITRUST L.J. 841, 852 (1989) ("Compulsory access, if it exists at all, is and should be very exceptional."); Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041, 1085–86 (1996).

Is the legacy-root server an essential facility to which ICANN must provide access? One court addressed this issue in a suit against NSI, though its decision leaves a number of issues unresolved. In *Thomas v. Network Solutions, Inc.*,[244] the plaintiffs were entities who had registered domain names through NSI. The D.C. Circuit held against them on the essential facilities claim, not because access to the root server was not essential (a question it did not decide), but because the plaintiffs in that case did not compete with NSI in a downstream market and so could not demonstrate a required element of an essential facilities claim.[245] By contrast, European competition law is not so restrictive, and a number of cases have been brought against registration authorities in Europe based on a quasi-essential facilities theory.[246]

A more likely essential facilities claim is one brought by a competitor. Under early pre-ICANN market structure, such a claim was fairly easy to envision. The government controlled the root zone file that was relied on by the alpha root server and all downstream copies of it. NSI controlled both the authoritative .com registry and was the exclusive registrar for .com and the other open gTLDs. Entry in the root zone file allowed firms to be registries. NSI's entry for .com meant that an entry in its database was necessary to permit others to access your web site by typing an alphanumeric URL that ended in .com. If your domain name was not in the registry whose address was found on the master list, no one relying on DNS servers in the legacy root could find you by entering that domain name.[247] If a plaintiff sought to compete as a registrar by taking registrations for .com, it would be stymied by NSI's refusal to enter such competing registrations in the only authoritative registry for .com listed in the root zone file. Thus, NSI would have denied access to a facility it controlled (the .com registry), essential to competition, to which it could feasibly have provided access, with the effect of perpetuating its dominance in a separate product market—the market for registration services.[248]

Over time, NSI was forced to allow other registrars to sell registrations. Even then, there were allegations that NSI's registry gave various sorts of preferential access to its registrar, and that the NSI registry's price (set in a contract with the U.S. Government) exceeded fair market

244. 176 F.3d 500 (D.C. Cir. 1999).

245. *Id*. at 510; *cf.* America Online, Inc. v. GreatDeals.Net, 49 F. Supp. 2d 851, 862–63 (E.D. Va. 1999) (finding that the complaint properly alleged that e-mail access to AOL subscribers was an essential facility, but was nonetheless dismissed because the plaintiff and defendant did not compete).

246. *See, e.g.*, E-mail from Cedric Manara, Professor, EDHEC Business School, to Mark Lemley, Professor of Law, University of California School of Law (Boalt Hall) (Jan. 16, 2002) (on file with the University of Illinois Law Review) (documenting cases brought in France, Belgium, and Spain).

247. They could, however, reach your web site with a browser by typing in the IP number. E-mail works slightly differently, and there are some e-mail programs that simply cannot send e-mail to an address at an IP number, but these are relatively rare. Although it is not part of the minimum specifications, most e-mail programs can send mail to an address of the form user@[129.171.97.1].

248. For such an argument, see Goldfoot, *supra* note 11, at 927–31.

value.[249] These problems stemmed from NSI's vertical integration. NSI controlled the .com registry, and also competed with other registrars in the market for registration services. It thus had the classic structure for an essential facilities claim. The obvious solution was to separate the registry's control from the registrar's control. Indeed, getting an agreement that NSI would divest itself of either the registrar or the registry by May 10, 2001 was supposed to be one of the DoC and ICANN's major achievements. When the time came, NSI threatened to divest itself of the registrar and then affiliate with another one, and ICANN backed down. It instead accepted VeriSign/NSI's proposal to divest itself of .org and .net within a few years while keeping .com. The government then further modified the agreement to require auditing of the "firewall" between the registry and the registrar and a few other antitrust-inspired changes.[250]

ICANN's control of access to the root raises different issues from NSI's because ICANN acts as neither a registrar nor a registry,[251] although it plans to take over direct control of the root zone from NSI at some point. ICANN has power over registries and (through them) registrars; its control is greatest over those seeking ICANN's approval to enter the legacy root. ICANN has at least one direct financial incentive to limit the number of gTLDs to the root. So long as there is a shortage of gTLDs, firms will pay ICANN substantial sums simply to be allowed to apply for consideration. Indeed, in 2000 ICANN was able to require applicants to pay it a nonrefundable $50,000 fee, "intended to cover ICANNs costs of receiving and evaluating the application, including performing technical, financial, business, and legal analyses, as well as ICANNs investigation of all circumstances surrounding the applications and follow-up items."[252] Forty-seven applicants purchased what amounted to expensive lottery tickets, but ICANN selected only seven to

249. *See, e.g.*, *Hearing on "Is ICANN's New Generation of Internet Domain Name Selection Process Thawting Competition?," Before the House Comm. on Energy & Commerce, Subcomm. on Telecommunications*, 107th Cong. (Feb. 8, 2001) (statement of A. Michael Froomkin, Professor of Law, University of Miami School of Law), *available at* http://www.house.gov/commerce/hearings/froomkin.htm (on file with the University of Illinois Law Review) (suggesting that increase in supply of domain names would lower prices and reduce incentives for cybersquatting).

250. *See supra* notes 129–39 and accompanying text.

251. Actually, ICANN has hosted the registries for new gTLDs as they come on stream. The reasons for this are unclear. Some have suggested it is a subsidy to the registries; others that ICANN wants an excuse to buy computers, or to learn how to run a registry in case it ever needs to rescue a failing one. ICANN's announcement was short on details, but describes it as a temporary measure. *See* IANA, *Report on Establishment of the .biz and .info Top-Level Domains*, *available at* http://www.iana.org/reports/biz-info-report-25jun01.htm (June 25, 2001) (on file with the University of Illinois Law Review) (noting that "[i]nitially, the nameservice for the domains will be operated by the IANA," which was by then a part of ICANN).

252. *See* ICANN, *New TLD Application Process Overview* § 2, *available at* http://www.icann.org/tlds/application-process-03aug00.htm (Aug. 3, 2000) (on file with the University of Illinois Law Review) (noting that "[t]he application fee is non-refundable and ICANN's only obligation upon accepting the application and fee is to consider the application").

receive a TLD.[253] The greater the number selected, the less leverage ICANN would have to require a similar payment from the next round of applicants.

Other than the premium it can demand from would-be entrants, however, it is debatable whether ICANN itself—as opposed to incumbent registries—has a financial incentive to limit the number of new entrants to the root. ICANN annually sets its financial needs and assesses income from registries and registrars, who pay according to various formulas that, in part, reflect their market shares. All other things being equal,[254] ICANN may have a financial incentive to increase the number of registrants, since that spreads the costs and increases the amounts it can levy without occasioning protest, which should argue for more TLDs since these should tend to increase total registrations. To the extent that new TLDs just shift a constant number of registrations around registries, ICANN should be neutral, unless the very small number of registries allows them to charge a premium price and lets ICANN demand part of that rent for itself. Only if new TLDs were to so significantly increase supply in the relevant market that it substantially depressed the prices charged by registries or registrars might ICANN's income stream be affected.[255] Because ICANN does not compete directly in either the registry or registrar markets, it does not conform to the classical structure of an essential facilities case.

ICANN's relationship with the alternate root operators presents a more complex issue in market definition and definition of market participants. On the one hand, the alternate root operators as a group are ICANN's true competitors in that they create opportunities (currently, tiny ones) for new TLDs and new registries. Plus, entrants in their roots do not pay ICANN's levies, giving ICANN a financial motive to fear growth in their market penetration—a growth that network effects suggest would be likely to take off once it reached some distant critical mass.[256] On the other hand, at present it is a little difficult to identify any

253. In contrast to the plaintiffs in *Smiley v. NeuLevel*, who proposed a highly plausible account of the .biz registration system as an illegal lottery, *see supra* note 23, it is unlikely that anyone could successfully argue that ICANN's selection process for new gTLDs was so random as to constitute a lottery. It may have been arbitrary and poorly thought out, but the process was not random.

254. One way in which they are not equal is the administrative cost of dunning large numbers of registrars. ICANN has been moving to a funding strategy that concentrates on registries because there are fewer of them. For example, ICANN's model contract with new gTLD registries contemplates having them collect ICANN's quarterly charges from registrars and remitting the sum to ICANN in place of the current practice by which ICANN bills registrars directly. *See* ICANN, *Proposed Unsponsored TLD Agreement* ¶¶ 3.14.1–5, *available at* http://www.icann.org/tlds/agreements/unsponsored/registry-agmt-11may01.htm (May 11, 2001) (on file with the University of Illinois Law Review).

255. There might also be administrative costs to ICANN associated with new TLDs. ICANN has clearly found it difficult to negotiate contracts with the new TLDs, some of which have, to date, taken nine months more than originally envisioned. Large numbers of TLDs might also have staffing implications.

256. *See generally* Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424 (1985); Mark A. Lemley & David McGowan, *Legal Implications of*

individual person or firm as ICANN's competitor. The alternate root operators work in a far more decentralized fashion than ICANN. There is no central policymaking body for the alternate roots as a group, and most of the major groups have only loose coordination bodies seeking to head off name collisions. So while the alternate root-based registries as a group are ICANN's competition, individually the operators are more like competition for ICANN-approved registries than for ICANN itself.[257]

The most important competitive relationship between ICANN and the alternate root operators arises from the competition for the name space. Traditionally, alternate root operators have worked with considerable (but not total) success to avoid creating "name collisions"[258]—two TLDs that use the same character string. They have also avoided creating TLDs that conflict with the legacy root, since users of the alternate root namespace also use the legacy root. Because ICANN does not recognize the legitimacy of the alternate roots, however, it has no compunction about approving TLDs that use a string already in use in an alternate root. Thus, for example, ICANN accepted and debated applications for the .web TLD from parties other than IODesign, which has been running .web as an alternate root since 1996,[259] although it ultimately chose not to assign that name to anyone. ICANN did, however, assign the .biz string to NeuLevel when there was already a very small functioning alternate root by that name.[260] In the view of the original .biz partisans, that made ICANN the "name collider." Whoever is right, both names cannot be in the same root, forcing alternate root operators to choose for the first time whether to abandon one of their own or to offer data conflicting with that used by the legacy root rather than simply supplemental to it.[261] Whatever the rights and wrongs of all this, it demon-

Network Economic Effects, 86 CAL. L. REV. 479 (1998) [hereinafter Lemley & McGowan, *Network Effects*].

257. The analysis might change in the unlikely event that, say, a large group of important national governments were to band together to form an alternate root and could persuade or require their domestic internet service providers and registries to support the move. This is, however, unlikely to happen. It would require a degree of international cooperation among national governments and ccTLDs far in excess of anything achieved so far in the domain name arena.

258. *See infra* note 304 and accompanying text.

259. *See* Image Online Design, Inc., *Frequently Asked Questions*, WEB™ INTERNET DOMAIN REGISTRY, *available at* https://www.webtld.com/info_faq.asp (last visited Aug. 18, 2002) (on file with the University of Illinois Law Review).

260. *See* A. Michael Froomkin, *.biz Is Tiny—or Is It?*, ICANNWATCH (June 19, 2001), *available at* http://www.icannwatch.org/article.php?sid=212 (on file with the University of Illinois Law Review) [hereinafter Froomkin, *.biz*] (discussing competing accounts of the size and viability of the "alternate" and preexisting .biz).

261. By September 2002, at least one of the alternate root providers had decided to abandon the alternate version of .biz and carry the ICANN version. *See* Posting of Bradley D. Thornton, Chief Technology Officer, The Pacific Root, Bradley@PacificRoot.com, to public@tlda.net (Sept. 14, 2002), *available at* http://www.freetld.net/pacroot-drops-biz.html (on file with the University of Illinois Law Review) (letter from one alternate root operator announcing he was dropping alternate .biz in favor of ICANN's).

strates that ICANN has a strong competitive effect on alternate TLDs with which its new entries to the root collide.

How would an essential facilities claim fare under this new structure? It seems clear that ICANN controls access to the system by which the overwhelming majority of registrants obtain domain names. At the same time, the existence of alternate roots may make it less likely that ICANN actually controls access to a facility essential to competition. If the barriers to duplicating—or more likely, supplementing—the root are not extraordinary, an essential facilities claim will founder on the first and second elements. Network effects may make it more difficult to set up a competing root that draws many customers,[262] but they will not make it impossible.[263] Further, even if the legacy root is essential at the root level, ICANN is not vertically integrated. Thus, even if ICANN's actions are consistent with a view that it seeks to punish anyone that tries to compete with it by running an alternate root, ICANN lacks the clear self-dealing incentive present in cases like *MCI* and *Otter Tail* because ICANN gets no direct financial benefit from choosing one registry over another.

A second problem with the essential facilities theory concerns the feasibility of providing access to the facility to everyone on reasonable and nondiscriminatory terms. If ICANN's concerns about the stability of a DNS with multiple gTLDs have any basis,[264] an essential facilities claim will founder on this fourth element. Even if those concerns are overstated, courts may well decide to defer to ICANN's expertise on the issue rather than take a chance with the stability of the DNS. As a result, even if ICANN is determined to control access to an essential facility, we are skeptical that courts will require it to open that facility to all comers because of concerns that doing so would be impractical.

262. *Cf.* Frankel, *supra* note 181, at 867 ("[T]he large Internet service providers' (ISPs) consensus to use a single root constitutes the foundation of ICANN's power. Most importantly, the tugging pressure of 'path dependence' in the case of ICANN is very great."). Nonetheless, Frankel concludes that that power is not without limits. *Id.*

263. For an early discussion, see Lemley & McGowan, *Network Effects*, *supra* note 256, at 555 n.323:

> Unlikely is not impossible, however. There are some reasons to believe that even here, network effects might not prevent effective competition between standards. First, the switch to a new domain name system need not be a complex one. NSI cannot claim to own the basic protocols that govern the Internet. It might be relatively straightforward, therefore, for a concerted group of large Internet users to switch their allegiance in a public way, causing others to follow suit. Second, and more important, it might be possible to run a new DNS system *alongside* the existing one, so that a company could be on both systems at once. If this is feasible, IBM could be accessed through ibm.com via NSI, and through a different (*or conceivably even the same*) domain name on a different system. Which system a user used would depend on how she accessed the Net. Lock-in concerns are significantly alleviated to the extent that users can simultaneously use more than one standard, as we have seen.

Id. Such parallel systems may be facilitated by the use of proxies—such as ISPs or browser software suppliers—who opt into such a parallel system on behalf of the user.

264. We discuss this issue in detail in the next section.

In short, it is unlikely that the legacy root will be determined to be an essential facility to which ICANN must provide access on reasonable and nondiscriminatory terms. However, this does not mean that ICANN will avoid liability for specific anticompetitive conduct. We discuss those issues in the sections that follow.

C. ICANN's Decision to Limit gTLDs and Restrict Registries

1. Exclusive Dealing

ICANN's decision to limit the number of new gTLDs created an artificial scarcity of domain names. It also limited the number of companies who could be registries, since the DNS as we know it assumes that there will be only one registry for each gTLD. ICANN's method of choosing registries presents rather serious antitrust issues.[265] ICANN's application document for would-be new gTLD registries,[266] and especially the accompanying "Criteria for Assessing TLD Proposals,"[267] made it clear that parties who dealt with ICANN's competitors would be rejected—even though those competitors' market share was almost trivial.[268] ICANN warned applicants that they should

> demonstrate specific and well-thought-out plans, backed by ample, firmly committed resources, to operate in a manner that preserves the Internet's continuing stability. The introduction of the proposed TLD should not disrupt current operations, nor should it create alternate root systems, which threaten the existence of a globally unique public name space.[269]

ICANN's demand that all applicants for approval as a new gTLD registry first forswear "alternate roots" is an exclusive dealing requirement.

Exclusive dealing arrangements are suspect under the antitrust laws because when entered into by a firm with a significant share of the market they may foreclose options to competitors, driving them from the market entirely or raising their costs.[270] For example, a dominant manufacturer may be able to "lock up" a large number of retail outlets by demanding that those outlets deal exclusively with it. As a result, compet-

265. For a related concern, that competition among gTLDs is still minimal, see Kesan & Shah, *supra* note 3, at 198–200.

266. *TLD Application Instructions*, *supra* note 115, § I20 ("ICANN absolutely requires stability in all aspects of new TLD registries.").

267. *Assessing TLD Proposals*, *supra* note 115.

268. ICANN, *Keeping the Internet a Reliable Global Public Resource: Response to New.net "Police Paper," available at* http://www.icann.org/icp/icp-3-background/response-to-new.net-09jul01.htm (July 9, 2001) (on file with the University of Illinois Law Review) (discussing the need for near-perfect universal resolvability); s*ee also ICANN Chief Issues Statement Criticizing Existence of Alternative Domain Name Roots*, 6 ELEC. COMM. & L. REP. 587 (2001).

269. *Assessing TLD Proposals*, *supra* note 115.

270. For a general discussion of the competitive risks of exclusive dealing arrangements, see 11 HERBERT HOVENKAMP, ANTITRUST LAW ¶ 1802 (1998) [hereinafter HOVENKAMP, ANTITRUST LAW].

ing manufacturers may find it difficult or impossible to place their goods in retail stores.

Not all or even most exclusive deals are anticompetitive, however. Exclusive dealing arrangements can also serve the useful purpose of guaranteeing a manufacturer an ongoing source of supply or a continuing outlet for distribution. This in turn permits the manufacturer to make investments on a long-term basis. It may also facilitate quality control and monitoring of sales outlets by the manufacturer.[271] As a result, exclusive dealing arrangements are judged under the Rule of Reason.[272] They are illegal only if the firm insisting on the agreement has a sufficient share of the market that the agreement will foreclose a significant amount of competition. Even then, the agreement can be justified if the defendant can show procompetitive benefits that outweigh any foreclosure.[273]

ICANN's decision to exclude companies who deal with alternate roots can also be characterized as monopolization under § 2 of the Sherman Act. As we will see, ICANN already has market power in the market for roots. Its exclusionary policy may help it to maintain that market dominance by making it harder for new competitors to grow. Because the standards for the two causes of action are similar, we treat them together in the sections that follow.

2. Market Power and Competitive Effects

Whether ICANN's exclusive dealing requirement is legal depends on ICANN's market power and on whether the exclusive dealing requirement is on balance procompetitive or anticompetitive. ICANN unquestionably has control over the legacy root. Virtually all gTLDs (measured by use[274]) are under ICANN's effective control, and ICANN's control over access to the legacy-root server creates rather substantial barriers to entry for alternate roots.

The continued existence of ccTLDs outside ICANN's direct control at first appears to complicate the market share determination. It is not clear, however, how much effective competition existing ccTLDs provide to existing gTLDs. Most ccTLDs are used predominantly by registrants in their home countries, although .tv, .md, and about two dozen others

271. *See* 11 *id*. ¶ 1802.

272. Exclusive dealing arrangements in goods are governed by § 3 of the Clayton Act, 15 U.S.C. § 14 (2000). Because registries provide services, not goods, the relevant law is provided by § 1 of the Sherman Act, 15 U.S.C. § 1. But the legal standards are largely the same in any event. *See generally* 11 HOVENKAMP, ANTITRUST LAW, *supra* note 270, ¶¶ 1802b, 1820b.

273. *See, e.g.*, Tampa Elec. Co. v. Nashville Coal Co., 365 U.S. 320, 334 (1961); 11 HOVENKAMP, ANTITRUST LAW, *supra* note 270, ¶ 1801i. For criticism of the balancing approach, and suggested alternatives, see 11 *id*. ¶ 1822b.

274. While groups such as New.net have a substantial number of gTLDs, they are not used by very many people.

have sought to market themselves as gTLD substitutes.[275] More to the point, ICANN has ultimate technical control over ccTLDs because it controls the root to which they are linked. Although it may seem that the political cost to ICANN of actually using its power over ccTLDs would be enormous, there are things ICANN can do to ccTLDs short of removing them from the root. For example, although ICANN has a contract with the U.S. government which requires ICANN to perform the "IANA function" of maintaining the root, including ccTLD information,[276] ICANN currently has a policy of refusing to make timely changes to the contact information and other data for any ccTLD that has not signed a contract with it.[277] Because the contracts ICANN wants ccTLDs to sign allow ICANN to demand payment that can increase at fifteen percent per year and confirm that ICANN may in some cases take a ccTLD away from its administrator, the existing ccTLDs have naturally been reluctant to sign these agreements.[278]

In any case, the proper market is the market for control of the roots (and therefore the ability to create new TLDs), not for control of individual TLDs (with the concomitant ability to control second-level domains). If a large majority of the ccTLDs were to band together and create a new alternate root, that new entity might have the clout to compete with ICANN; there is no reason, however, to believe that they are willing or able to do so. Estimates of how many people use existing alternate roots vary, but the numbers of people using true alternate name resolution services is probably well under one percent of all Internet users, and the number of domain name registrants in the true alternate roots is very small indeed. Even today, what is presumed to be the largest "alternate" registry, .web, boasts only about 26,000 registrations.[279] The small take-up is hardly surprising, given that the alternate roots suffer from a classic

275. In addition to the ccTLDs that offer nonresidents second-level registrations akin to .com, a number of ccTLDs permit foreigners to register third- or fourth-level names, e.g., name.co.ccTLD. These are usually of far less interest to nonresident buyers unless they are defensively registering a trademarked name around the world.

276. *See supra* note 61 and accompanying text.

277. *See* Posting of Elisabeth Porteneuve, Elisabeth.Porteneuve@cetp.ipsl.fr, to council@dnso.org (Sept. 13, 2002), *available at* http://www.dnso.org/clubpublic/council/Arc11/msg00035.html (Sept. 13, 2002) (on file with the University of Illinois Law Review); ccTLD Constituency, Communiqué Presented to the ICANN Public Forum in Marina del Rey § 5 (Nov. 12, 2001), *available at* http://www.wwtld.org/communique/ccTLDMdR_communique_12Nov2001.html (on file with the University of Illinois Law Review); *see also* A. Michael Froomkin, *dotcx says 'ICANN Threatens the Stability of the Internet'*, ICANNWATCH (July 2, 2001), *available at* http://www.icannwatch.org/article.php?sid=229 (on file with the University of Illinois Law Review). One example of the exercise of this power is ICANN's refusal to permit the .eu domain to be added to the DNS until the EU signs a registry agreement with ICANN. *See, e.g.*, David McGuire, *ICANN Has Final Say on Dot-EU Internet Domain—Update*, NEWSBYTES, (Mar. 26, 2002), *available at* http://www.webprowire.com/exec/doc404/47663 (on file with the University of Illinois Law Review).

278. *See* ICANN, *Proposed ccTLD Sponsorship Agreement (.au)*, *available at* http://www.icann.org/cctlds/au/proposed-sponsorship-agmt-04sep01.htm (Sept. 4, 2001) (on file with the University of Illinois Law Review).

279. Froomkin, *.biz*, *supra* note 260.

network effect,[280] and that a registration in an alternate root is of relatively little value in the absence of a critical mass of fellow users who can access that root. The existence of this network effect, coupled with ICANN's control over the dominant root, makes ICANN's exclusive dealing particularly effective. By denying alternate roots the right to participate in running gTLDs in the legacy root, ICANN keeps those alternate roots marginalized, and makes it far less likely that they will ever achieve that critical mass. The foreclosure in question here is not substantial in percentage terms simply because ICANN's control is so complete.[281] But it effectively forecloses the most likely source of competition for ICANN's legacy root.

ICANN's exclusionary conduct toward competitors is exemplified in its treatment of New.net. Despite New.net's limited market penetration, ICANN has singled it out for vituperative criticism and crafted new policies designed to ensure that potential customers understand their New.net registrations will never be recognized in the ICANN root. First, ICANN's Chief Policy Officer accused New.net of "breaking the Internet" and "selling snake oil."[282] Then, ICANN's President and CEO authored a paper attacking New.net's bona fides and legitimacy that he (eventually[283]) labeled a "discussion draft."[284] Then, without any warning, ICANN announced that a slightly revised version of the paper was official ICANN policy, and that no "bottom-up" discussions were required because the paper was merely articulating long-standing policy rather than making it.[285] In fact, however, the paper contained a number

280. On the role of network effects in cementing the control of the legacy root, see Lemley & McGowan, *Network Effects*, *supra* note 256, at 553–55.

281. The absence of a significant foreclosure percentage often dooms exclusive dealing claims. *See* 11 HOVENKAMP, ANTITRUST LAW, *supra* note 270, ¶ 1821d1. But the defendant rarely has the almost complete control over the market that ICANN has in this case. We do not think that ICANN's success in dominating the market renders its reliance on exclusive dealing arrangements less problematic.

282. Kevin Murphy, *ICANN Strikes Back, Refuses to Be Strong-Armed by New.net*, NETWORK BRIEFING DAILY (July 12, 2001), *available at* http://www.softwareuncovered.com/news/nbd-20010712.html (on file with the University of Illinois Law Review) (comments of ICANN Chief Policy Officer Andrew McLaughlin); Letter from Daniel Scott Schecter, Esquire, Latham & Watkins, to ICANN Board of Directors (July 16, 2001), *available at* http://www.icann.org/correspondence/schecter-letter-to-icann-16jul01.htm (on file with the University of Illinois Law Review).

283. There was some confusion on this as ICANN initially published the paper on its web page without any sign that it was a draft, a personal statement, or for discussion. After a brief storm of protest, ICANN added a preface from ICANN President and CEO M. Stuart Lynn saying it was his attempt to restate existing policy and the technical basis for such policy. *See* A. Michael Froomkin, *ICANN's Lynn on Alternative Roots*, ICANNWATCH (May 29, 2001), *available at* http://www.icannwatch.org/article.php?sid=180 (on file with the University of Illinois Law Review).

284. ICANN, *Discussion Draft: A Unique, Authoritative Root for the DNS*, *available at* http://www.icann.org/stockholm/unique-root-draft.htm (May 28, 2001) (on file with the University of Illinois Law Review).

285. *See* M. Stuart Lynn, *Statement on Completion of "A Unique Authoritative Root for the DNS" (ICP-3)*, *available at* http://www.icann.org/icp/icp-3-background/lynn-statement-09jul01.htm (July 9, 2001) (on file with the University of Illinois Law Review); s*ee also* Jonathan Weinberg, *How ICANN Policy Is Made*, ICANNWATCH (July 10, 2001), *available at* http://www.icannwatch.org/article.php?sid=241 (on file with the University of Illinois Law Review).

of new policies designed to make clear to the Internet community that ICANN had no intention of allowing New.net domains into the root, and indeed would feel free to create colliding TLDs if and when it chose. These conclusions seemed both novel and controversial.[286]

ICANN needed a new policy because New.net presented a substantial potential threat to ICANN's monopoly over the TLD namespace. Were New.net to achieve critical mass in a TLD, ICANN would find it difficult to create a colliding TLD without facing accusations that it, as the latecomer to that name, was the one "breaking the Internet" by creating name conflicts for a substantial installed base of users. Worse (from ICANN's point of view), New.net grabbed some of the most popular TLDs, often after asking potential users to vote on which TLDs they would like to see created. From ICANN's perspective, as a self-described guardian of the public trust, it is wrong to allow an entrepreneur to grab whatever attractive names it wants rather than taking its chances along with other applicants to ICANN.[287] And indeed, New.net has chosen an ever-increasing number of TLDs that collide with long-standing "true" alternate roots.

286. One of us joined Professor Jonathan Weinberg in filing a reconsideration request in which we suggested that new policies of this sort should be made by ICANN's "bottom-up" policy-creation process and not by executive fiat. *See* Jonathan Weinberg & A. Michael Froomkin, *Request for Reconsideration 01-5*, *available at* http://www.icann.org/committees/reconsideration/weinberg-request-08aug01.htm (Aug. 8, 2001) (on file with the University of Illinois Law Review); *see also* Jonathan Weinberg & A. Michael Froomkin, *Reconsideration Request: ICANN's Authoritative Root Paper*, ICANNWATCH (Aug. 8, 2001), *available at* http://www.icannwatch.org/article.php?sid=286 (on file with the University of Illinois Law Review) (describing request). ICANN rejected that argument, contending that the policies were not new but derived from past practice and the White Paper. *See* ICANN, *Reconsideration Request 01-5, Recommendation of the Committee*, *available at* http://www.icann.org/committees/reconsideration/rc01-5.htm (Jan. 18, 2002) (on file with the University of Illinois Law Review). The Reconsideration Committee did recommend "the adoption of the practice that designation of future documents within the ICP series be upon Board endorsement, so as to avoid future controversies regarding whether they are authoritative," but did not choose to recommend subjecting the alternate root paper to that discipline. *Id.* The ICANN board adopted the Reconsideration Committee's recommendation at a special meeting of the board held by teleconference on February 12, 2002. *See* ICANN, *Preliminary Report, Special Meeting of the Board*, *available at* http://www.icann.org/minutes/prelim-report-12feb02.htm (Feb. 12, 2002) (on file with the University of Illinois Law Review).

287. Some of these operators and their supporters assert that their very presence in the marketplace gives them preferential right to TLDs to be authorized in the future by ICANN. They work under the philosophy that if they get there first with something that looks like a TLD and invite many registrants to participate, then ICANN will be required by their very presence and force of numbers to recognize in perpetuity these pseudo TLDs, inhibiting new TLDs with the same top-level name from being launched through the community's processes.

No current policy would allow ICANN to grant such preferential rights. To do so would effectively yield ICANN's mandate to introduce new TLDs in an orderly manner in the public interest to those who would simply grab all the TLD names that seem to have any marketplace value, thus circumventing the community-based processes that ICANN is required to follow. For ICANN to yield its mandate would be a violation of the public trust under which ICANN was created and under which it must operate. Were it to grant such preferential rights, ICANN would abandon this public trust, rooted in the community, to those who only act for their own benefit. Indeed, granting preferential rights could jeopardize the stability of the DNS, violating ICANN's fundamental mandate.

See Lynn, *ICP-3*, *supra* note 20.

An example of ICANN's special opposition to New.net occurred in connection with ICANN's Annual Meeting in November 2001. In response to ICANN's general call for sponsorship, New.net sent in a $5,000 fee, which would have entitled it to display its logo at a coffee break during the meeting, and to distribute company material at the sponsors' table. ICANN returned the check, saying that New.net was not welcome because it did not support the authoritative root. As ICANN President and CEO Stuart Lynn put it, "we place bounds around whom we accept as sponsors. And New.net does not fit the package."[288]

ICANN's reaction to New.net can usefully be compared to its treatment of non-ASCII internationalized domain names (IDN).[289] IDNs will likely create nonunique domain names, at least from the users' perspective. Furthermore, some IDN solutions considered by the technical community would have posed a threat to ICANN's monopoly of the root. ICANN supported efforts to create non-ASCII domain names, despite the danger of nonuniqueness, and encouraged developments that do not threaten the centrality of the legacy root.[290] Although the decision

288. Posting of Danny Younger, Chair, ICANN General Assembly, DannyYounger@cs.com, to ga@dnso.org (Oct. 27, 2001), *available at* http://www.dnso.org/clubpublic/ga-full/Arc08/msg02851.html (on file with the University of Illinois Law Review). The Business Constituency of the DNSO also excluded New.net on the grounds that the constituency is closed to registrars. *See* Kieren McCarthy, *ICANN Caught Red-Handed*, THE REGISTER (Oct. 25, 2001), *available at* http://www.theregister.co.uk/content/6/22482.html (on file with the University of Illinois Law Review). New.net, however, is not an ICANN-accredited registrar, and thus would also be barred from the DNSO Registrars' constituency. *See* ICANN, *ICANN-Accredited Registrars*, *available at* http://www.icann.org/registrars/accredited-list.html (last modified Aug. 12, 2002) (on file with the University of Illinois Law Review); ICANN, *Registrars' Constituency By-Laws*, *available at* http://www.icann-registrars.org/pdfs/bylaws1.pdf (last modified Oct. 9, 2001) (on file with the University of Illinois Law Review).

289. The DNS currently uses a very limited character set composed of certain case-insensitive ASCII characters. Thus, domain names can only contain the roman alphabet, integers, and dashes; WWW.LAW.TM is identical to WwW.lAw.Tm. There is no provision for Han or Kanji characters in domain names, nor even an "ö" with an umlaut. A full conversion of the DNS to a system that could handle multiple character sets would have required either a wholesale reengineering of the unknown number of DNS applications that rely on ASCII, or required some means to flag non-ASCII domain names and have them resolved by a different means.

290. Internet standards tend to emerge de facto from the marketplace, such as the Adobe document format, or by agreement within the relevant standards body, in this case the Internet Engineering Task Force (IETF). In November 1999, the IETF created an IDN working group to wrestle with the thorny question of setting an IDN standard, and in September 2000, the ICANN board resolved that once a single standard emerges from the relevant standards body, all the competing encoding schemes should conform to the standard. *See* ICANN, *Minutes of Special Meeting*, Resolutions 00.77–.80, *available at* http://www.icann.org/minutes/minutes-25sep00.htm (Sept. 20, 2000) (on file with the University of Illinois Law Review).

VeriSign deployed an IDN encoding scheme it labeled a "testbed." *See* VeriSign, *Find An Internationalized Domain Name*, *available at* http://global.networksolutions.com/en_US/name-it/ml-index.jhtml (last visited Aug. 19, 2002) (on file with the University of Illinois Law Review) ("Internationalized domain names are being offered as part of a trial period or 'testbed.' Resolution of internationalized domain names has not yet occurred, and, although anticipated at a later stage of the testbed, cannot be guaranteed. Future changes in internationalized domain name technology standards may invalidate some of the names registered during the testbed.").

ICANN reacted by warning that any deployment of an IDN solution prior to the decision of the IETF must remain an experiment, *see* ICANN, *Comment on NSI Registry Multilingual Domain Name Testbed*, *available at* http://www.icann.org/announcements/comment-25aug00.htm (Aug. 25, 2000) (on

is not yet final, the Internet Engineering Task Force's (IETF's) current proposal, "Internationalizing Domain Names in Applications (IDNA),"[291] will not call for a change in the way that the DNS resolves domain names.[292]

Unlike some possible alternatives, IDNA does not work like an alternate root. Instead, it uses special zones carved out of the legacy root.[293] ICANN anticipated this result, which resembles the "testbed" solution being offered by VeriSign, when it inserted reservations into its contracts with the new gTLDs that prevented the new TLDs from registering any second-level domains with a dash "in the third and fourth character positions."[294] To prevent cybersquatting of IDN names, the IETF proposal states that ICANN will choose the two letter prefix when the standard goes into effect.[295]

Within the IETF, the IDNA proposal has been controversial for two reasons. First, it is an inelegant hack. Worse, IDNA does not accommodate all character sets equally, and deals erratically with domain names composed of mixtures of two character sets.[296] Furthermore, the

file with the University of Illinois Law Review) (warning VeriSign and others that existing IDN schemes much be considered temporary), even though VeriSign's method did not create an alternate root. So far, this strategy seems to be working. While the IETF's IDN working group might have agreed on an IDN scheme that routed around ICANN, *see e.g.*, JOHN C. KLENSIN, INTERNATIONALIZING THE DNS—A NEW CLASS (Internet Eng'g Task Force Internet Draft, Dec. 4, 2000), *available at* http://www.i-d-n.net/draft/draft-klensin-dnsclass0e.txt (on file with the University of Illinois Law Review), the IETF proposal that currently seems most likely to be adopted will pose no threat to ICANN.

291. *See* PATRIK FALTSTROM ET AL., INTERNATIONALIZING DOMAIN NAMES IN APPLICATIONS (IDNA) (Internet Eng'g Task Force Internet Draft, May 24, 2002), *available at* http://www.ietf.org/internet-drafts/draft-ietf-idn-idna-10.txt (on file with the University of Illinois Law Review) [hereinafter IDNA].

292. Instead, IDNA would make client software such as e-mail programs and browsers do all the work of transforming non-ASCII characters (e.g., Kanji) to a set of ASCII characters before sending a DNS request to resolve a domain name. The user will see the Japanese characters but before the message gets onto the Internet the local software will covert it into something that the DNS can understand: a two-character prefix followed by two dashes and a load of gobbledegook (e.g., "bq--1k2n4h4b"). *See id.*

293. *Id*. Other coding schemes can be imagined, some with a real potential for the creation of de facto competing and colliding name spaces in nonromance character sets. At present it does not seem likely that any of these will be deployed widely enough to matter.

294. *See, e.g.*, ICANN, *Proposed Unsponsored TLD Agreement: Appendix K* § C, *available at* http://www.icann.org/tlds/agreements/unsponsored/registry-agmt-appk-26apr01.htm (last modified Apr. 26, 2001) (on file with the University of Illinois Law Review). Although labeled "proposed" on the website this is in fact part of the final agreement, see ICANN, *.biz Registry Agreement*, *available at* http://www.icann.org/tlds/agreements/biz/ (May 11, 2001) (on file with the University of Illinois Law Review).

295. Technically, the proposal delegates this task to IANA, which currently functions as a wholly owned subsidiary of ICANN. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 86–87, 103.

296. Many important language-based and script-based mappings are not covered in IDNA and must be handled outside the protocol. For example, names that are entered in a mix of traditional and simplified Chinese characters will not be mapped to a single canonical name. Another example is Scandinavian names that are entered with U+00F6 (LATIN SMALL LETTER O WITH DIAERESIS) will not be mapped to U+00F8 (LATIN SMALL LETTER O WITH STROKE).

FALTSTROM ET AL., *supra* note 291, § 6.6.

reliance of a client-based (i.e., browser and email program) solution means that users will inevitably get unexpected, seemingly random, results when using software that is not properly configured, and there may be little the DNS servers can do about it.[297] For Chinese users in particular, the level of user confusion may turn out to be higher than anything created by New.net.[298]

From ICANN's viewpoint, however, the IDNA proposal means it dodged a bullet. The actual domain name registration remains an ASCII-character registration in the ICANN-controlled root. While the domain names may be conflicting in the eye of the beholder, from ICANN's perspective they remain "unique" and under its ultimate control—although the same might be said of New.net names to the extent they include a fourth-level, name.tld.new.net component. It is notable that ICANN has been willing to accommodate IDNA but not New.net or any alternate root.

ICANN obviously benefited from its action to foreclose any chance that new gTLD registries would in any way assist alternate roots. ICANN's authority and revenues flow from its contracts with registrars and registries. By ensuring that the alternate roots remain shut out from the biggest players, ICANN exacerbates the network effects that keep its primary competition small.[299] Registries in the ICANN system that would not be interoperating with alternate roots also benefit, since they are protected from that competition. On the other hand, registrars and customers lose out, since there are fewer domain names to sell, and less competition between registries. As regards quasi-alternate roots like New.net, ICANN's exclusive dealing requirement is akin to the sort of "defensive leveraging" condemned by the D.C. Circuit in the *Microsoft* case.[300] ICANN benefits from limiting the outlets for companies like New.net not because it hopes to enter their market, but because it wants to prevent them from threatening its existing monopoly. ICANN's exclusive dealing requirement therefore seems anticompetitive on its face.

3. Procompetitive Justifications

Exclusive dealing arrangements entered into by monopolists that foreclose significant competition are presumptively illegal. Even so, the defendant will escape antitrust liability if it can demonstrate a legitimate

297. *See, e.g.*, Posting of Adam M. Costello, idn.amc@nicemice.net, to idn@ops.ietf.org (June 4, 2002), *available at* http://www.imc.org/idn/mail-archive/msg06705.html (on file with the University of Illinois Law Review).

298. *See* XIAODONG LEE ET AL., TRADITIONAL AND SIMPLIFIED CHINESE CONVERSION (Internet Eng'g Task Force Internet Draft, June 28, 2001), *available at* http://www.i-d-n.net/draft/draft-ietf-idn-tsconv-00.txt (on file with the University of Illinois Law Review).

299. *See* Lemley & McGowan, *Network Effects*, *supra* note 256, at 553–55 (discussing network effects first realized by NSI).

300. *See* United States v. Microsoft Corp., 253 F.3d 34, 74–78 (D.C. Cir. 2001); Robin Cooper Feldman, *Defensive Leveraging in Antitrust*, 87 GEO. L.J. 2079, 2096–2100 (1999).

procompetitive justification for its behavior.[301] In this case, whether ICANN can make such a showing will depend on the technical merits of its argument that alternate roots create instability.[302] At best, however, ICANN's technical arguments can justify its opposition to alternate roots. No technical argument can justify a refusal to deal in any way with anyone who operates or facilitates an alternate root.

The case for ICANN's technical rationalization of its policy against alternate roots relies on the weight of establishment technical opinion, especially the opinion of the influential Internet Architecture Board (IAB). There is, however, a case to be made that the rationale is pretextual. Proponents of alternate roots certainly disagree with it, some commentators have rejected it,[303] and ICANN's own protocol standards body recently refused to endorse the IAB opinion.

The technical case against alternate roots rests in large part on the belief that domain names should always resolve to the same resource[304] regardless of who is accessing it and where they are located. If competing roots have name collisions for a TLD, i.e., if there is more than one registry for a given TLD taking competing registrations which are then reflected in different DNS name resolution hierarchies, then this uniqueness is lost. Instead of everyone seeing the same site when they typed www.kafka.law into their browser, results will vary. What result a user will get will ordinarily depend on someone's choice, but that someone may be the user or someone upstream from the user, depending on who selects the DNS. So far, however, the main consequence of alternate roots is that they create a need either for user education, or for the DNS equivalent of area codes. In a world of thriving competitive roots with name collisions, however, even users who control their DNS service sometimes might experience unexpected results if, for example, they were to use a web-based e-mail form to send mail. Mail to fred@kafka.law on Fred's machine might go somewhere different than e-mail to that address sent from somewhere else. Indeed, to the extent that Internet services rely on intermediate machines for their transport via domain names rather than IP numbers, the routing of the data may vulnerable to any routing errors induced by inconsistent DNS resolution en route.

301. *See, e.g.*, *Microsoft*, 253 F.3d at 75.

302. *See Hearing on Domain Names*, *supra* note 117 (testimony of Dr. Vinton Cerf); *cf.* Brian Carpenter, Internet Architecture Board, *Technical Comment on the Unique DNS Root*, *available at* http://www.icann.org/correspondence/iab-tech-comment-27sept99.htm (Sept. 27, 1999) (on file with the University of Illinois Law Review).

303. *See, e.g.*, Milton L. Mueller, Competing DNS Roots: Creative Destruction or Just Plain Destruction? (2000) (unpublished manuscript), *available at* http://istweb.syr.edu/~mueller/tprc-2001-mueller.pdf (on file with the University of Illinois Law Review) (arguing that alternate roots should be permitted as "a healthy outlet for inefficiency or abuses of power by the dominant root administrator").

304. Usually, but not always, a resource at a single IP number.

None of these dangers occur, however, in the absence of TLD name collisions. A merely supplementary alternate root does not present the same dangers, so long as there are no name collisions within it either. Even here, however, users may be frustrated if, much like a person trying to reach a New.net TLD from the legacy root today, they click on a link and get an error message because their DNS does not recognize the existence of the supplementary TLD.

An additional, potentially more serious, problem is "cache poisoning," which can occur without TLD name collisions, and indeed without alternate roots. The DNS uses a number of shortcuts to allow DNS servers to cache data and quickly resolve domain names to IP numbers. These shortcuts prevent every computer from having to query the same root server every time a URL is entered or a domain name is sent. Rather, a copy of the current version of the root zone file is "cached" in a local computer, and those who need to look up an address can do so at the local computer. Strange things can happen, however, when not all computers in the network carry the same information concerning which name server is authoritative for a particular domain or even TLD. To save time, caches are set to collect additional information beyond what is immediately necessary for a given resolution request. So-called cache poisoning occurs when, in the process of acquiring one set of name resolution information, a querying computer also happens to collect some extra data connecting a name (or TLD) to different machine than the one the user would ordinarily expect. Suppose, for example, that Alice's computer ordinarily uses the legacy root. A malicious person sets up DNS records that point amazon.com to his bookstore rather than to the real one to divert sales from the famous brand. If he can arrange for his computer to pass along IP number information linking his store to the www.amazon.com domain name, anyone whose DNS server has come into contact with his misleading information will cache it, causing anyone relying on that server to get the wrong store when they type "www.amazon.com" into their browser.[305] These problems can also occur

305. This is the infamous 'Kashpureff hack' which relied on a vulnerability in BIND:

> This vulnerability exists in all versions of BIND prior to version 4.9.6 and version 8.1.1. It allowed an intruder to cause a victim name server to query a remote name server controlled by the intruder. The remote name server would return bogus information to the victim name server. The bogus information would be cached on the victim name server for a period specified by the TTL field of the record returned by the remote name server. Very simply, this attack allowed the intruder to point the victim name server's host name IP address mapping to an alternate IP address of the intruder's choice. Eugene Kaspureff [sic] used cache poisoning to divert the traffic from www.internic.net to www.alternic.net.

Nalneesh Gaur, *Securing Name Servers on UNIX*, 68 LINUX J. (1999), *available at* http://www2.linuxjournal.com/lj-issues/issue68/3691.html (on file with the University of Illinois Law Review); *see* Doug Sax, DNS Spoofing (Malicious Cache Poisoning) (Nov. 12, 2000) (unpublished manuscript), *available at* http://www.0100101110101101.org/home/glasnost/project/tmp/cache-pollution/DNS_spoof.htm (on file with the University of Illinois Law Review).

without any malice.[306] When there are competing roots using the same TLD, a similar problem can happen on a larger scale. Suppose there are two competing versions of .biz. Alice, being unaware of this, would, like most people, normally use the one in the legacy root. But, if Alice's DNS server happens to get data from a machine that uses an alternate version of .biz, it may innocently pass along the name resolution info for that alternate authoritative name server. Alice's DNS server caches it, and the next time she seeks a .biz name it will route the query to the alternate root's server rather than the legacy one. Not only might this cause unexpected results, but it is highly likely to cause inconsistent ones for Alice since her cache may at a later time revert to data pointing to the legacy root's server. For Alice, that would mean that some web pages in the .biz domain would seem to vanish and appear at random, while others changed unpredictably. ICANN argued that the increase in the use of alternate roots might worsen the problem.[307]

The significance of these various technical factors remains controversial. In May 2000, the IAB, which functions as the IETF's steering committee, weighed in against alternate roots, stating in RFC 2826:

> To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore, it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority.
>
> Put simply, deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers.[308]

M. Stuart Lynn's paper for ICANN echoed this language.[309]

Ordinarily, a paper from the IAB would be considered all but authoritative. Nevertheless, supporters of alternate roots attacked RFC 2826 as political, and noted that as it was labeled "Informational," it had not been subjected to the IETF's consensus-building processes used for true standards. Subsequently, others proposed ways of organizing alter-

306. *See, e.g.*, Posting of Mike Batchelor, mikebat@tmcs.net, to jwa@jammed.com (July 17, 2001), *available at* http://lists.jammed.com/incidents/2001/07/0081.html (on file with the University of Illinois Law Review).

307. Lynn, *ICP-3*, *supra* note 20.

308. Carpenter, *supra* note 302.

309. *See* Lynn, *ICP-3*, *supra* note 20. Arguably the TLD cache poisoning problem stems in substantial part from ICANN's decision to deploy TLD strings already in use in the alternate roots. On the other hand, there are a lot of small alternate roots, and it is not obvious that they ought necessarily to have priority in the name space. None of these issues has yet been ventilated in the ICANN decision-making process other than in ICANN President and CEO M. Stuart Lynn's unilateral statement. *See id.*

nate roots with a degree of coordination that, they argue, would not create the problems that worry the IAB.[310] Their proposals have not been adopted by the IETF, however, and indeed the IETF has apparently refused to allow them to proceed to discussion. Most recently, ICANN's own Protocol Supporting Organization (PSO) was asked to opine on RFC 2826's condemnation of alternate roots. It refused to endorse it, instead issuing an artful statement:

> The Internet DNS currently operates using a Single Authoritative Root Server System. Although, it would be technically possible to devise and standardize a fully compliant alternative multiple root server system, there appears no technical reason for changing from the present working system, as this would require the development of a new set of protocols for use by the DNS.[311]

The PSO's statement is artful because the "new set of protocols" to which it refers might mean any one of three things. In theory, the new protocols might be primarily *social* rather than *technical*: ICANN might find a way to coexist with alternate roots and agree to avoid name collisions. Or, radically decentralizing technical protocols might be created that allowed users, or their software, to select among multiple roots much like people dial area codes to select among otherwise identical telephone numbers.[312] Or, ICANN could adopt new protocols that added new capabilities to ICANN's existing hierarchical root. These new capabilities would allow new functions akin to alternate roots, although they would require new user software and would leave the DNS firmly in ICANN's control.[313]

It is not clear how courts would evaluate all of this in the context of an exclusive dealing antitrust claim. On the one hand, it is well established that only procompetitive arguments may be considered as legitimate business justifications. ICANN is not free to argue that its foreclosure of competition was a good thing because competition itself is

310. *See, e.g.*, SIMON HIGGS, ALTERNATIVE ROOTS AND THE VIRTUAL INCLUSIVE ROOT (Internet Eng'g Task Force Internet Draft, May 2001), *available at* http://www.higgs.com/publications/id/draft-higgs-virtual-root-00.txt (on file with the University of Illinois Law Review); SIMON HIGGS, ROOT SERVER DEFINITIONS (Internet Eng'g Task Force Internet Draft, Feb. 2001), *available at* http://www.higgs.com/publications/id/draft-higgs-root-defs-00.txt (on file with the University of Illinois Law Review); Karl Auerbach, Delving into Multiple DNS Roots (n.d.) (unpublished manuscript), *available at* http://www.cavebear.com/tmp/multiple-roots.doc (last visited Sept. 3, 2002) (on file with the University of Illinois Law Review).

311. Protocol Supporting Organization, ICANN, *Statement*, *available at* http://www.pso.icann.org/PSO_Statements/PSO-Statements-28September2001.txt (Sept. 28, 2001) (on file with the University of Illinois Law Review).

312. *See supra* note 310 and accompanying text.

313. For example, M. Stuart Lynn's proposal for experimental alternate roots relies on the use of the creation of new 'class identity' identifiers, and software to resolve the new class(es). The structure of the DNS, and the hierarchical control over the root, would remain exactly as it is today. *See* Lynn, *ICP-3*, *supra* note 20.

undesirable.[314] Nor would ICANN be free to argue that its refusal to accept bids from anyone who ran an alternate root could be justified on technical grounds, as placing a formerly alternate root into the legacy room solves the very technical problems that alternate roots allegedly can cause. On the other hand, courts are willing to consider certain justifications for the regularization of competition in circumstances in which a market might not otherwise form. Thus, in *Broadcast Music, Inc. v. CBS*,[315] the Court permitted a copyright owners cartel that provided licenses to millions of songs at a single flat rate. The Court reasoned that the cartel itself was procompetitive, since it eliminated transactions costs that would otherwise be prohibitive, and effectively "made" a new market.[316] Similarly, some courts have permitted stock exchanges and trade associations to set up internal rules governing who can participate and excluding outsiders where such rules were necessary to let the market function effectively.[317] Such restrictions are not always permitted, however, and the courts will inquire in detail into whether the restriction on competition is actually necessary.[318] Even assuming that the refusal to permit interconnection with alternate roots may have a reasonable technical justification, the refusal to consider doing business with anyone who runs or deals with an alternate root cannot necessarily rely on that technical justification. ICANN's refusal to accept as a registry any company that operates or deals with an alternate root can be justified only if there is reason to believe that ICANN's action would empower those companies to cause tangible harm to the legacy root—a harm more substantial than simply legitimating the alternate root.

In summary, it is unclear whether the desire for DNS uniformity justifies ICANN's exclusion of alternate roots from the list of potential registries. Certainly, the antitrust cases suggest that ICANN's asserted justifications will be subject to searching scrutiny on their merits. To the extent ICANN can convincingly present a technical need to consolidate the DNS in a single root, the law will likely defer to that technical justification. By contrast, if someone could demonstrate that consolidation is not necessary for technical reasons, ICANN's insistence on excluding al-

314. *See* Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 689–90 (1978) (citing early cases as foreclosing "the argument that because of the special characteristics of a particular industry, monopolistic arrangements will better promote trade and commerce than competition").

315. 441 U.S. 1 (1979).

316. *Id.* at 22–23.

317. *See, e.g.*, Chi. Bd. of Trade v. United States, 246 U.S. 231 (1918); *cf.* 2 HOVENKAMP ET AL., *supra* note 221, § 35.3 (discussing legitimate reasons to impose membership restrictions on standards bodies and related groups).

318. *See, e.g.*, NCAA v. Chi. Bd. of Regents, 468 U.S. 85, 88 (1984) (rejecting the NCAA's justification for limits on television coverage of college football); United States v. Realty Multi-List, Inc., 629 F.2d 1351, 1369–87 (5th Cir. 1980) (conducting an exhaustive inquiry into a real estate association's membership rules, and concluding that they violated the Rule of Reason because the organization had market power and the rules were insufficiently related to legitimate business concerns); *cf.* Silver v. N.Y. Stock Exch., 373 U.S. 341, 343, 364–65 (1963) (holding that stock exchange violated antitrust laws by excluding members without providing them notice and a hearing).

ternate roots would be problematic under the antitrust laws. Even if ICANN's technical arguments are warranted, they do not justify exclusion of anyone who deals with an alternate root unless there is reason to believe that those applicants will use their position to undermine the stability of the legacy root.

D. The Wait List Service

Another example of exclusive dealing, but one that is easier to evaluate, involves the new "Wait List Service" (WLS) proposed by VeriSign[319] and accepted, with some amendments, by ICANN.[320] There is a market for the identification and registration of domain names that expire and are not renewed. In appropriate cases, intellectual property owners, cybersquatters, and companies wishing to purchase a generic domain name may want to be notified when a particular name becomes available so they can register it. A vibrant competition exists to supply this demand, with companies like SnapNames selling a notification service.[321] In 2002, VeriSign (the .com registry) proposed to eliminate this competition by having ICANN create a sole-source WLS.[322] The proposed WLS would replace the competition by registrars to identify and precommit domain names with a central service offered for a fee by VeriSign.[323]

The WLS is an exclusive dealing arrangement with particularly obvious anticompetitive consequences. An existing competitive market would be eliminated and replaced with a monopoly granted by ICANN to VeriSign. Neither ICANN nor VeriSign has offered any plausible technical need for a centralized service, and the fact that a decentralized system is already in operation without obvious problems strongly suggests that there is no such technical need. There are, however, certain advantages to a uniform service. Specifically, the first person put on the new wait list will be guaranteed to get the domain name when it becomes available, while in the existing competitive market a request placed with one company may not be filled if a competing wait-list registrar gets the name first. An exclusive arrangement therefore offers more certainty—at least to the person who happens to be first on the wait list—than a competitive market. But that sort of "regularization" of the market—insulating the lucky winner from the vagaries of competition—is unlikely to serve as a legitimate procompetitive justification for eliminating com-

319. *See* VeriSign, *Domain Name Wait Listing Service*, *available at* http://www.icann.org/bucharest/vgrs-wls-proposal-20mar02.pdf (Mar. 20, 2002) (on file with the University of Illinois Law Review) [hereinafter VeriSign, *WLS*].

320. *See* ICANN, *Preliminary Report, Special Meeting of the Board*, *available at* http://www.icann.org/minutes/prelim-report-23aug02.htm (Aug. 23, 2002) (on file with the University of Illinois Law Review).

321. SnapNames' services are available at http://www.snapnames.com (last visited Oct. 8, 2002).

322. *See* VeriSign, *WLS*, *supra* note 319, at 3.

323. *See id.* at 3–5.

petition. And an exclusive dealing arrangement that forecloses substantial existing competition without any valid procompetitive justification will likely be illegal under the Rule of Reason.

It may be that intellectual property owners prefer this arrangement because they assume that they will likely end up first on the list. What is less clear about the WLS is what incentive ICANN has to endorse such a scheme. ICANN does not appear to benefit financially from granting VeriSign a monopoly over wait-list domains. The ICANN General Counsel's report recognizes the competitive problems with the VeriSign approach, and ameliorates the concerns by: (1) refusing to permit VeriSign's existing partner, SnapNames, to get first preference in registering names on the WLS; and (2) requiring VeriSign to charge a price based on the cost of providing the service.[324] This seems to be a case in which ICANN is not an active participant in a conspiracy to monopolize a market, but has agreed for unknown reasons (conceivably pressure from the IP constituency or fear of legal action by VeriSign) to facilitate VeriSign's effort to monopolize the market. If so, the real culprit here is VeriSign. We consider its liability in part IV. In the absence of any motive to restrict competition, ICANN itself will likely not be liable merely for adopting such an exclusive deal if it can offer a reasonable business reason for its conduct.[325] If, on the other hand, it is found to have conspired with VeriSign, its lack of a financial motive will not protect it.

E. The Uniformity of the UDRP

Competition is not only about selling goods or services at the lowest price. For competition to be free and unfettered, companies must be able to compete as well on the nature and quality of the products they sell. Competition in the breakfast cereal industry, for example, requires not just that many different companies produce corn flakes, but that different companies be free to experiment with different types of cereal. Companies in that industry clearly establish market niches in part on their willingness to serve different types of customers with different types of cereals.

So too with goods or services of any type, including domain names. Registrars in a competitive marketplace will attempt to take business away from each other not only by lowering their price, but also by offering different and better services than their competition. Because the registrars' customers are domain name registrants, registrars in a competitive market might be expected to compete by offering rights or benefits that make their domain names more valuable. Among the things that

324. Louis Touton, General Counsel, ICANN, *Second Analysis of VGRS's Request for Amendment to Registry Agreement* § 2.5, *available at* http://www.icann.org/minutes/report-vgrs-wls-22aug02.htm (Aug. 22, 2002) (on file with the University of Illinois Law Review).

325. *See* HOVENKAMP, ANTITRUST POLICY, *supra* note 224, § 7.6e.

registrars would compete over are the way, speed, and skill with which they would resolve domain name trademark disputes. Indeed, those registrars that predate ICANN had different policies for dealing with such disputes.

The UDRP short-circuited this competition. ICANN required all registrars to agree to impose a uniform dispute resolution policy on their registrants. By doing so, ICANN entered into a vertical agreement restricting nonprice competition on one axis.[326] This in and of itself is not necessarily an antitrust problem. Manufacturers regularly impose nonprice restraints on their distributors or retailers; doing so may legitimately serve to prevent free-riding and is normally legal.[327]

More troubling is the means by which the UDRP was adopted. ICANN did not develop the UDRP itself and impose it on the registrars. Rather, a group of registrars themselves banded together and, using a draft policy from the WIPO as a model, drafted the initial provisions with input from intellectual property owners. These registrars then collectively presented the draft to ICANN, which adopted it with only minor changes. Thus, it appears that the UDRP was not in fact merely a vertical agreement imposed by ICANN on its customers, but actually reflects a horizontal agreement among the registrars themselves to limit competition in dispute resolution procedures. Horizontal agreements are much more worrisome, particularly where (as here) they are entered into by the largest companies in the market.[328] ICANN appears not to have been the driving force in drafting the policy, but rather a "ringmaster" employed by the registrars to enforce their own agreement.[329] The issue is more complicated, however, because the registrars in turn have no direct incentive to insist on uniform dispute resolution. Rather, they were motivated by pressure from the trademark owners (who acted with the endorsement-in-principle of the U.S. government as expressed in the White Paper), backed by the threat of lawsuits and a fear that the trademark constituency could prevent both registrar competition and the development of new gTLDs altogether. Michael Palage, the head of the Registrars' DNSO Constituency, famously said that "[t]he trademark lobby must be placated because of its potential ability and inclination to

326. There is now a second dispute resolution policy, called STOP, which ICANN mandated for the start-up period of new gTLDs such as .biz. The existence of a second policy does not reflect competition, however. Rather, STOP has been uniformly imposed by ICANN on all registrars in the new gTLD space for the preregistration period. It differs from the UDRP only in that it gives trademark owners new rights during the "sunrise" period when the new TLDs are first opened to registrants, and that the registries can select among the ICANN-approved providers of dispute services rather then being required to accredit all of them.

327. *See, e.g.*, Bus. Elec. Corp. v. Sharp Elec. Corp., 485 U.S. 717 (1988); Cont'l T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36 (1977).

328. *See supra* note 133 for a listing of participants, including NSI.

329. *See* Thomas G. Krattenmaker & Steven C. Salop, *Anticompetitive Exclusion: Raising Rivals' Costs to Achieve Power over Price*, 96 YALE L.J. 209, 238–40, 260–62 (1986) (describing this as the "cartel ringmaster" theory).

bankrupt new registrars and wreck havoc on their registrant databases."[330]

Horizontal agreements to restrict nonprice competition are not necessarily illegal per se. Rather, they will be given a "quick look" to determine whether there are legitimate procompetitive justifications for the agreement. If there are arguable justifications, the agreements will be analyzed under the Rule of Reason.[331] Here, the obvious purpose of the agreement is to limit cybersquatting. There is strong evidence that the UDRP was enacted at the behest of intellectual property owners who likely had the political power to prevent the adoption of any new gTLDs unless the registrars agreed to restrict cybersquatters. Certainly the effect of the UDRP has been to punish cybersquatters, in part by establishing procedures that have systematically favored intellectual property owners even in doubtful cases.[332] But even granting that cybersquatting is a bad thing, collusion among erstwhile competitors to treat it uniformly is not necessarily legal. The Supreme Court has made it clear that justifications for horizontal agreements must be procompetitive, not just good social policy. It has rejected justifications for cartels based on the idea that competition itself will lead to bad results.[333] Only if the standardization at issue is necessary to *promote* competition will it be permitted.[334]

The clear effect of the UDRP is to eliminate competition that otherwise would have existed between registrars about how to resolve disputes. That competition may well have been undesirable as a matter of social policy.[335] But as a matter of antitrust law, it does not matter.

330. *See* Posting of Judith Oppenheimer, joppenheimer@icbtollfree.com, to I-strategy@list.adventive.com (Apr. 6, 2001), *available at* http://www.judithoppenheimer.com/pressetc/adentive.html (on file with the University of Illinois Law Review) (quoting remark by Palage at a January 10, 2000 Small Business Administration meeting on Domain Name Issues).

331. *See, e.g.*, Cal. Dental Ass'n v. FTC, 526 U.S. 756, 759 (1999).

332. For empirical evidence that this has occurred, see Geist, *supra* note 200; Mueller, *supra* note 200.

333. *See, e.g.*, Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 689–90 (1978) ("The early cases also foreclose the argument that because of the special characteristics of a particular industry, monopolistic arrangements will better promote trade and commerce than competition. That kind of argument is properly addressed to Congress and may justify an exemption from the statute for specific industries, but it is not permitted by the Rule of Reason.") (citation omitted).

334. Thus, technical standard-setting organizations are generally not liable under the antitrust laws for eliminating competition, because there is normally a technical need for a single standard to make products compatible. *Cf.* Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041 (1996). Setting a uniform product standard in the absence of such a technical need would raise antitrust concerns.

335. There is a great deal of academic debate over whether certain forms of regulatory competition result in a "race to the bottom," in which regulatory regimes are rewarded for being inefficiently lax. *See, e.g.*, ROBERTA ROMANO, THE GENIUS OF AMERICAN CORPORATE LAW 14–31 (1993); Ehud Kamar, *A Regulatory Competition Theory of Indeterminacy in Corporate Law*, 98 COLUM. L. REV. 1908, 1947–48 (1998); Lynn M. LoPucki & Sara D. Kalin, *The Failure of Public Company Bankruptcies in Delaware and New York: Empirical Evidence of a "Race to the Bottom,"* 54 VAND. L. REV. 231, 237 (2001); Jonathan R. Macey & Geoffrey P. Miller, *Toward an Interest-Group Theory of Delaware Corporate Law*, 65 TEX. L. REV. 469, 474–76 (1987). While registrars are not governments, one might reasonably fear a similar effect in a competitive regime, because registrants (registrars' customers) might

There does not seem to be the sort of market-making necessity for the UDRP that ICANN has asserted as a justification for excluding alternate roots.[336] And ICANN cannot prevail by explaining why competition among registrars is itself a bad idea.

ICANN's possible liability for adopting the UDRP is related to antitrust concerns about its policy on alternate roots as well. Alternate roots are not subject to the UDRP because they have not contracted with ICANN. They therefore constitute a potential source of competition in registration policies, one that ICANN is foreclosing. Thus, neither policy should be considered in isolation. If the standardized UDRP agreement is illegal, ICANN is liable regardless of whether it was the motivating force behind the policy. Even reluctant or coerced coconspirators violate the antitrust laws by entering into the conspiracy.[337] Further, the standard-setting cases seem to suggest that standard-setting organizations themselves violate the antitrust laws even if the illegal activity was conducted by members acting without authorization from the organization.[338]

The potential plaintiffs harmed by the UDRP are primarily the registrants subjected to it.[339] Any possible plaintiff would, however, need to

prefer to externalize any costs of their infringement rather than be subject to any sort of dispute resolution scheme at all.

The matter is complicated in this case by the fact that the U.S. Congress passed the Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d) (2000), the same month the UDRP was adopted. Thus, dispute resolution competition among registrars would have been limited in any event by the legal backstop: trademark owners were and remain free to go to court rather than use any private dispute resolution system. For this if for no other reason, the ACPA may serve a useful purpose. *But see* Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 320–36 (2002) (criticizing the ACPA as unnecessary).

Further, there is a great deal of trenchant criticism of the procedures that the UDRP uses. *See, e.g.*, Froomkin, *Partial Cures*, *supra* note 139, at 670–78; Helfer & Dinwoodie, *supra* note 3, at 189–237; Geist, *supra* note 200; Mueller, *supra* note 200; Port, *supra* note 200, at 1112–17; Elizabeth G. Thornburg, *Fast, Cheap and Out of Control: Lessons from the ICANN Dispute Resolution Process*, 6 J. SMALL & EMERGING BUS. L. 191, 207–24 (2002). *But see* Stephen J. Ware, *Domain-Name Arbitration in the Arbitration-Law Context: Consent to, and Fairness in, the UDRP*, 6 J. SMALL & EMERGING BUS. L. 129, 161–65 (2002) (defending UDRP procedures). It is at least possible that competition between dispute-resolution systems would have led to a less problematic process.

336. *See supra* notes 204–07 and accompanying text.

337. Calnetics Corp. v. Volkswagen of America, Inc., 532 F.2d 674, 682 (9th Cir. 1976) ("The involuntary nature of one's participation in a conspiracy to monopolize is no defense."), *cert. denied*, 429 U.S. 940 (1976); *cf.* MCM Partners, Inc. v. Andrews-Bartlett & Assocs., 62 F.3d 967, 973 (7th Cir. 1995) (citing *United States v. Paramount Pictures, Inc.*, 334 U.S. 131, 161 (1948), as well as several later cases, to support its holding that a § 1 conspiracy "is not negated by the fact that one or more of the coconspirators acted unwillingly, reluctantly, or only in response to coercion").

338. *See, e.g.*, Am. Soc'y of Mech. Eng'rs v. Hydrolevel Corp., 456 U.S. 556, 570–71 (1982) (holding that ASME violated antitrust laws where a member sent a threatening letter to one of its competitors on ASME letterhead, even though the member acted without actual authority in sending the letter); 2 HOVENKAMP ET AL., *supra* note 221, § 35.8.

339. eResolution, the arbitration services provider driven out of the market because it was seen as less "plaintiff-friendly" than its competitors, might seem to be a potential plaintiff injured by the policy. *See* David G. Post, *eResolution out of UDRP Business*, ICANNWATCH (Nov. 30, 2001), *available at* http://www.icannwatch.org/article.ph/p?sid=484 (on file with the University of Illinois Law Review) (noting eResolution folded, citing shrinking market share due to the complainants' preference for providers they thought would enhance their chances of winning). Because eResolution lost business due

overcome a difficult standing hurdle. Although there have been several thousand UDRP cases filed to date, there are millions of domain names. Therefore, the average registrant faces only a minimal chance of being subject to a UDRP proceeding. In the absence of any specific reason to believe that a UDRP proceeding was imminent,[340] it could easily be argued that the registrant's injury was so remote and speculative as to lack the necessary concreteness to give the registrant standing.[341] Indeed, in the absence of some threatened or actual UDRP proceeding, as an abstract matter the balance of probabilities is similar to the probability of being subject to a chokehold that the Supreme Court held was insufficient in *City of Los Angeles v. Lyons*.[342] This standing problem is unlikely to be cured by a class action filing. Unlike the mootness doctrine, the constitutional requirement of standing lacks an exception for "capable of repetition yet evading review"—at least for cases where "a plaintiff lacks standing at the time the action commences."[343] In this view, only a confirmed cybersquatter or someone who was able to freeze the UDRP action before it came to a conclusion[344] would have a sufficiently strong showing of concrete harm from the UDRP to overcome the standing hurdle, and few would choose to label themselves cybersquatters.[345]

In contrast, a domain registrant who had lost a UDRP decision before an arbitral panel and then sought to prevent transfer of the name by going to court would be in a strong position to claim antitrust damages from the costs of defending the UDRP. However, there is reason to doubt whether a court would hear a claim for injunctive protection against future harm even on the basis of a completed UDRP action. This claim might also be subject to the rebuttal that any future damage is only speculative.[346] At least one court has held that because domain name

to the rational independent decision of thousands of trademark owners to choose a plaintiff-friendly service, any such claim would have to allege that the registrars conspired to set the rules in a way that eliminated a competitor in a market that did not yet exist at the time the rules were made. Because eResolution became a UDRP dispute resolution provider after the rules were established, it seems more likely that it signed its own death warrant by refusing to cater sufficiently to the desires of trademark owners. The result may not be fair, but it does not appear to preclude competition in the dispute resolution provider market.

340. A threatening demand letter from a trademark holder might suffice.

341. City of Los Angeles v. Lyons, 461 U.S. 95, 105–10 (1983).

342. *Id.*

343. *See* Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 190 (2000) (citing *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 (1998)).

344. The registrant might secure a preliminary injunction from the court, or the UDRP arbitrators might (but also might not) stay the proceeding themselves. *See* ICANN, *Rules for Uniform Domain Name Dispute Resolution Policy* § 18(a), *available at* http://www.icann.org/dndr/udrp/uniform-rules.htm (last modified Feb. 5, 2002) (on file with the University of Illinois Law Review) ("In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.").

345. For one thing, the ACPA provides for up to $100,000 statutory damages for cybersquatting. 15 U.S.C. §§ 1117(d), 1125(d)(1) (2000).

346. *See Lyons*, 461 U.S. at 109.

registrants "voluntarily" submit to UDRP decisions, and because they have a right to *de novo* review in a court, they cannot demonstrate actual injury from the promulgation of the UDRP.[347]

On the other hand, a registrant who goes to court to block the UDRP action before the decision is rendered will have standing to challenge its future application. At that moment, the claim that the UDRP case causes a direct and foreseeable harm is neither moot nor lacking in standing. Unless the UDRP action is stayed almost immediately by the court, however, it is likely to conclude well before any antitrust litigation is even begun in earnest.

Although registrars are possible defendants, some registrars are also potential plaintiffs. A registrar who wished to offer customers a domain name not subject to the UDRP could seek injunctive relief under the Sherman Act. The registrar would ask the court to invalidate the part of the registrar's contract with ICANN in which ICANN requires the registrar to impose the UDRP on its customers.[348]

Registrars, and others who take part in ICANN's activities, also face liability for their attempts to have ICANN make rules. We turn to this possible liability in the next part.

IV. LIABILITY FOR PETITIONING ICANN

In addition to the state action and governmental immunity doctrines, private actors who petition the government in an effort to influence it to act are immune from antitrust liability even if the actions they seek are anticompetitive. This *Noerr-Pennington* immunity[349] creates a sort of penumbra around the state action doctrine in which anticompetitive petitioning may take place without antitrust liability. The fundamental basis for this petitioning immunity is the First Amendment right to petition.[350] As Justice Scalia put it, it would be "peculiar in a democracy, and perhaps in derogation of the constitutional right 'to petition the government for a redress of grievances' . . . to establish a category of lawful state action that citizens are not permitted to urge."[351] Efforts to petition the government are immune from antitrust liability unless those efforts amount to no more than a "sham."[352]

In this case, though, registries, registrars, registrants, and trademark owners are not petitioning the government itself. Rather, they are peti-

347. *See* Bord v. Banco de Chile, 205 F. Supp. 2d 521, 523–24 (E.D. Va. 2002).

348. Some registrars also may have claims that ICANN's approval of VeriSign's WLS proposal will have anticompetitive effects, although whether this claim is better directed at VeriSign alone or VeriSign and ICANN together could be debated.

349. *See, e.g.*, United Mine Workers v. Pennington, 381 U.S. 657 (1965); E. R.R. Presidents Conference v. Noerr Motor Freight, Inc., 365 U.S. 127 (1961).

350. On the source of petitioning immunity, see McGowan & Lemley, *supra* note 15, at 307–14.

351. City of Columbia v. Omni Outdoor Adver., Inc., 499 U.S. 365, 379 (1991).

352. *See* Prof'l Real Estate Investors v. Columbia Pictures Indus., Inc., 508 U.S. 49, 56 (1993).

tioning ICANN, a private corporation acting under the authorization of the government. There is of course no immunity for "petitioning" a purely private entity; were it otherwise, cartels and other agreements between competitors would all be immune.[353] But petitioning ICANN is perhaps an intermediate case, since ICANN's existence is authorized by governmental policy, and there is a plausible argument that it is a state actor for antitrust purposes.[354]

The closest analogue is *Allied Tube & Conduit Corp. v. Indian Head, Inc.*,[355] which involved efforts to influence the National Fire Protection Association (NFPA), a private standard-setting body whose model codes were routinely enacted into law unchanged by state legislatures.[356] The Court held that Allied Tube was not immune from liability for petitioning the NFPA because the NFPA lacked the public accountability of a truly governmental body:

> Whatever *de facto* authority the Association enjoys, no official authority has been conferred on it by any government, and the decisionmaking body of the Association is composed, at least in part, of persons with economic incentives to restrain trade. . . . [W]here, as here, the restraint is imposed by persons unaccountable to the public and without official authority, many of whom have personal financial interests in restraining competition, we have no difficulty concluding that the restraint has resulted from private action.[357]

To the extent that ICANN lacks public accountability,[358] has no official authority,[359] and has a financial interest to restrain competition,[360] it is a private body and those who petition it will enjoy no special immunity.[361]

353. *See, e.g.*, Raymond Ku, *Antitrust Immunity, the First Amendment and Settlements: Defining the Boundaries of the Right to Petition*, 33 IND. L. REV. 385 (2000). *But see* Eurotech, Inc. v. Cosmos European Travels Aktiengesellschaft, 189 F. Supp. 2d 385, 391–94 (E.D. Va., 2002) (holding that the UDRP is sufficiently public to entitle UDRP plaintiffs to the same *Noerr-Pennington* immunity granted to litigants in federal courts). If, contrary to the hypothesis animating this paper, a court were to find that ICANN is a state actor, arguably *Noerr-Pennington* immunity might be extended to those petitioning ICANN itself.

354. As noted above, however, we ultimately find that argument unpersuasive. *See supra* notes 351–53 and accompanying text.

355. 486 U.S. 492 (1988).

356. *Id*. at 495.

357. *Id*. at 501–02.

358. Many arguments have been made along these lines. *See, e.g.*, Froomkin, *Wrong Turn*, *supra* note 3; Liu, *supra* note 6.

359. On this more complicated issue, see *supra* notes 31–34 and accompanying text. *See generally* Froomkin, *Wrong Turn*, *supra* note 3.

360. *See supra* notes 112–15 and accompanying text (describing ICANN's benefit from restraining competition by alternate roots). ICANN seems to lack a similar financial incentive to enforce the UDRP, except to the extent its adoption placates trademark owners who would otherwise have the power to block ICANN initiatives.

361. *See* Sessions Tank Liners, Inc. v. Joor Mfg., Inc., 17 F.3d 295, 298–301 (9th Cir. 1994) (finding that misrepresentations to a quasi-public standard-setting organization could violate the antitrust laws where the organization acted in an administrative rather than a legislative capacity). For a similar argument relating to NSI's predecessor, the InterNIC, see Stephen J. Davidson & Nicole A. English, Applying the Trademark Misuse Doctrine to Domain Name Disputes (1996) (unpublished manu-

As with the state action doctrine, merely determining that immunity does not apply is only the beginning of the inquiry. Courts must still apply the normal principles of antitrust law to determine whether the act of petitioning is itself anticompetitive. We consider the liability of petitioners in two different circumstances: the WLS and the UDRP.

A. VeriSign and the WLS

As noted above,[362] VeriSign has petitioned ICANN to replace an existing competitive market with an ICANN-mandated monopoly granted to VeriSign. Such a deal could well violate the antitrust laws. And while VeriSign would be immune under the *Noerr-Pennington* doctrine if it got the government to grant it such a monopoly, given ICANN's private status, VeriSign will face antitrust liability for persuading a private company in a position of power to grant it control over a market.

B. The UDRP

As noted above,[363] ICANN adopted the UDRP under substantial lobbying pressure by registrars, who in turn were under substantial pressure from trademark owners to do something about cybersquatting. The private defendants in any antitrust claim based on the UDRP may be either the registrars themselves or conceivably the trademark owners who induced the registrars to act.

As for the registrars themselves, they can loosely be grouped into a few categories. First, there are the registrars who actively participated in drafting or approving the UDRP. Second, there are the other registrars accredited before the UDRP took effect in October 1999. Third, there are registrars whom ICANN accredited after the UDRP was already in place. Since one is no more required to be an ICANN registrar than one is required to register a domain name in the ICANN root, from a liability perspective, all three groups are equally liable for their participation in any ICANN-UDRP conspiracy.[364] This may come as a particular shock to firms that had themselves accredited either for bragging rights, or to register their own domains, but do not carry on much or any business with the public. The liability analysis for the registrars will likely track that for ICANN discussed above,[365] since they are allegedly part of the same cartel.

script), *available at* http://www.cla.org/trademark%20misuse.pdf (on file with the University of Illinois Law Review).

362. *See supra* Part III.D.

363. *See supra* Part III.E.

364. *See supra* note 337 (citing cases supporting the notion that all three groups would be held liable under antitrust laws).

365. *See supra* notes 358–61 and accompanying text.

Alternatively, one might suggest that certain trademark owners themselves were liable for petitioning ICANN to help them out by setting favorable dispute resolution rules. Particular trademark owners might be considered consumers of domain names, and thus ultimately in competition with cybersquatters who want to register those same domain names. But no particular trademark owner has power in such a market. Whether trademark owners could be held liable for collectively lobbying a private entity for favorable rules is less clear. Joint actions by groups like the International Trademark Association (INTA), an important participant in ICANN, will at least be subject to antitrust scrutiny. But simply asking collectively for a favorable policy is not illegal. Only if the trademark owners went further, threatening to use their collective power to influence the market (say, by boycotting any process that did not treat them favorably) would competitive concerns arise.

What is clear is that if private actors do not enjoy petitioning immunity for their contacts with ICANN, they will have to take more care than they have to date to conform their behavior to the requirements of antitrust law. Groups of registrars, registries, or potential registries must take particular care about agreeing together on a course of conduct; § 1 of the Sherman Act imposes greater restrictions on horizontal agreements to restrict trade than the restrictions on unilateral conduct we have discussed so far.

V. POLICY IMPLICATIONS

By delegating policy-making authority to ICANN, a private actor, without putting in place any real mechanisms for accountability, the government has created some unanticipated legal problems. It seems clear that the government itself could operate the legacy root in a way that excludes alternate roots without violating the antitrust laws. Similarly, the government should be able to impose a uniform domain name dispute resolution policy on registrars and registrants without antitrust liability,[366] although this might require legislation. It could also delegate these tasks to a private entity like ICANN without antitrust liability if the government affirmatively set the policy and actively supervised ICANN's implementation of it. Under *Noerr* and the government immunity doctrines, the price of unsupervised delegation is antitrust scrutiny. And it is not clear that ICANN and those in a position to influence it will survive that scrutiny. To avoid antitrust liability, ICANN will have to consider carefully both its policy regarding alternate roots and likely its UDRP as well. These policies are not necessarily illegal, but ICANN will have to offer evidence that they are on balance good for competition—

366. As one of us has noted elsewhere, however, the nature of the UDRP might raise constitutional concerns if compelled directly by a state actor. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 93–101, 132–38.

something that to date it has not been obliged to do. At a minimum, ICANN's policies will be subject to increased scrutiny, and likely to protracted antitrust litigation.[367]

This may not be a desirable result as a policy matter. There are plausible reasons to concentrate control of the root, or at least control over entry to the root, in one entity. Decentralized roots increase the chance of collisions or incompatibilities between TLDs operated by different entities. While there may be decentralized solutions to this problem, it is a risk that we might decide is not worth taking. Similarly, the UDRP performs a function many people value: it gives trademark owners and domain name registrants a cheap and quick way to resolve disputes over alleged cybersquatting. The astonishing number of UDRP proceedings to date—nearly 6,000—is a testament both to the continuing seriousness of the issue and the relative cost and speed of the UDRP compared to judicial action.[368] The UDRP has problems—it may not give respondents enough process or gather enough information, and there is recent evidence that it is systematically biased in favor of trademark owners.[369] But we might decide that a cheap and rapid dispute resolution system is worth giving up some certainty that the outcomes are correct.

The problem, though, is that as it stands presently "we" do not get to make any such decision. Whether to allow alternate roots, and how to design a domain name dispute resolution policy, are important policy questions. They may be decisions we ought to leave to the market, an approach that would allow alternate roots and would permit registrars to design nonuniform dispute resolution policies. Alternatively, the government may decide that it should displace the market outcome in the interest of ensuring the Internet's stability or dealing with the problem of cybersquatting.[370] In either case, the decision will have been made by an

367. While we have focused our attention on U.S. antitrust law, this conclusion is even more robust with respect to foreign antitrust statutes. EU antitrust law has no analog to the *Noerr-Pennington* or state action doctrines, and is somewhat more likely than U.S. antitrust law to compel access to essential facilities. *See, e.g.*, 2 HOVENKAMP ET AL., *supra* note 221, § 45.5b. And because ICANN's reach is global, it will be subject to multiple, overlapping antitrust rules. *See generally* Andrew T. Guzman, *Antitrust and International Regulatory Federalism*, 76 N.Y.U. L. REV. 1142 (2001) (discussing the intractability of the overlap problem in international antitrust).

368. A search for "Anticybersquatting Consumer Protection Act" on Westlaw in September 2002 turned up 106 cases. By contrast, in the same period UDRP arbitrators decided 5,932 cases involving 9,842 different domain names. ICANN, *Statistical Summary of Proceedings Under Uniform Domain Name Dispute Resolution Policy*, *available at* http://www.icann.org/udrp/proceedings-stat.htm (Oct. 1, 2002) (on file with the University of Illinois Law Review). Hundreds more were pending. For an argument that the ACPA was unnecessary, in part because of the existence of the UDRP, see Sherry, *supra* note 335, at 355–56.

369. *See* Froomkin, *Wrong Turn*, *supra* note 3, at 93–101; *supra* notes 328–30 and accompanying text.

370. For an argument that the questions ICANN is addressing are policy questions that are public in nature, see Liu, *supra* note 6, at 604. For even stronger suggestions that privatizing the network may be inefficient, see Brett Frischmann, *Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Mar-*

institution that is accountable to the public in some form—either the market, in which consumers can "vote with their wallet," or the government, which voters can change on election day.[371] Accountability is desirable because it permits error correction. If it turns out that the UDRP system has structural flaws, for example—as appears to be the case[372]—those flaws can be identified and corrected. By contrast, current policy abdicates this decision to a private, unelected entity that is also not subject to normal market constraints. If it turns out that ICANN makes the wrong decision, there is currently nothing to be done.

The government should take a more active role in setting domain name policy, either by running the DNS itself, or by actively supervising its delegates, or by making an affirmative decision to let the market work unfettered. If the government will not step in to do one of these things, antitrust law can fill an important part of the void.

ket, 2 COLUM. SCI. & TECH. L. REV. 1 (June 10, 2001), *available at* http://www.stlr.org/cite.cgi?volume=2+article=1; Kesan & Shah, *supra* note 3.

371. Another possibility is that the problem might be turned over to an existing, or newly created, international treaty body. If the root were administered by or under the direct supervision of a foreign or international governmental body, that body would likely enjoy immunity as a foreign sovereign, see Foreign Sovereign Immunities Act, 28 U.S.C. §§ 1330, 1602–1611 (2000), so long as the body is acting in a "public" rather than a "commercial" manner. *See* 2 HOVENKAMP ET AL., *supra* note 221, § 35.7a3. If the governmental body is immune, *Noerr-Pennington* immunity would apply to those who petition such a body. On the other hand, if the root remains in private hands, or if a government body in control of the root engages in unprotected "commercial" acts, the mere fact that the petitioning occurs outside the United States would not prevent the application of U.S. antitrust laws. *See id.* § 41.2 (discussing the extraterritorial reach of the Sherman Act).

372. *See, e.g.*, Geist, *supra* note 200; Mueller, *supra* note 200. Among the more obvious structural problems are the short time frame for response, which prevents many respondents from answering at all or from retaining a lawyer; the lack of an appeal procedure; and the fact that complainants get to select the private company that will arbitrate the dispute, giving those companies every incentive to cater to complainants (trademark owners) in deciding cases. For more detail on these procedural deficiencies, see Froomkin, *Wrong Turn*, *supra* note 3, at 96–101; Froomkin, *Partial Cures*, *supra* note 139.