Site Finder and Internet Governance

Jonathan Weinberg*

* Professor of Law, Wayne State University. I am grateful to Michael Froomkin, Mark Lemley, David Maher, Milton Mueller, and Jessica Litman for their comments, and to Susan Crawford and Bret Fausett for answering questions along the way. None of them, of course, is responsible for anything I say here. This essay reflects developments taking place through 30 November 2003.

Site Finder and Internet Governance

Jonathan Weinberg

INTRODUCTION

ON SEPTEMBER 15, 2003, VeriSign, Inc.—the company that operates the databases that allow internet users to reach any internet resource ending in ".com" or ".net"—introduced a new service it called Site Finder. Less than three weeks later, after widespread protest from the technical community, at least three lawsuits, and a stern demand from ICANN (the Internet Corporation for Assigned Names and Numbers, which has undertaken responsibility for managing the internet domain name space), VeriSign agreed to shut Site Finder down.[1] In between those dates the internet community saw a passionate debate over the roles of ICANN, VeriSign, and the internet's technical aristocracy in managing the domain name space.

VeriSign has charged that its opponents' reactions were the product of "obsolete thinking" that would disable it from "build[ing] a commercial business."[2] ICANN, for its part, is seeking to enact a procedure under which top-level domain name registry operators such as VeriSign must seek ICANN's approval before offering new services or taking any "significant actions that...could affect the operational stability, reliability, security or global interoperability of...the Internet."[3] Some see fault on all sides: "It's hard to say," writes one commentator, "in this case *who* is being more anti-competitive, ICANN or VeriSign."[4]

In this essay, I will try to unpack the Site Finder story. In Part 1, I will

---

1. VeriSign has suggested, though, that Site Finder is not easy in its grave and may yet be revived. See Declan McCullagh, "VeriSign to Revive Redirect Service?" *CNET News.Com* (15 October 2003), <http://news.com.com/2100-1038-5092133.html >.
2. Charles Cooper, "The Cultural Divide and the Internet's Future" *CNET News.Com* (16 October 2003), <http://news.com.com/2008-7347-5092590.html>.
3. "Staff Manager's Issue Report on the Need for a Predictable Procedure for Changes in the Operation of TLD Registries" *ICANN* (19 November 2003), <http://www.icann.org/gnso/issue-reports/registry-svcs-report-19nov03.htm> ["Staff Manager's Issue Report"].
4. A. Michael Froomkin, "Is VeriSign Contemplating a Sherman Act Claim Against ICANN?" *ICANNWatch* (8 October 2003), <http://www.icannwatch.org/article.pl?sid=03/10/08/2116252> [emphasis in original].

explain what VeriSign did, and how others reacted. In Part 2, I will address the Site Finder service from a technical standpoint, and in Part 3 from a regulatory one. I will assume that the reader has basic familiarity with ICANN and the operation of the internet domain name system. Finally, in Part 4, I will examine the Site Finder dispute from an institutional standpoint.

The answer, I urge, is not simply to beef up ICANN control; we don't need ICANN as a heavy-handed regulator of registry services generally. At the same time, the internet's own processes of self-correction may not be sufficient in cases like this one to preserve a stable basis for technical progress. One of the reasons ICANN was created was to take over U.S. government oversight aimed at preventing VeriSign's predecessor-in-interest from abusing its monopoly control over internet naming resources. Much went wrong at that institutional moment; the concept of ICANN was likely flawed from the start.[5] But if the creation of ICANN is to have done any good at all, then it is important for that body to be able to act where VeriSign is seeking to monetize its dominant position in ways that threaten the principles on which the internet was built.

*

1.

THE DOMAIN NAME SYSTEM (DNS) allows users to gain access to internet resources using a variety of internet applications—web browsers, email clients, FTP clients or others. When any of these applications seeks access to a resource identified by a domain name, the user's computer queries a name server, and that name server in turn queries a top-level domain registry database. If the queried name does not exist in the registry database, then—until September 15, 2003—all but a few small top-level domains returned a "no such address" answer (NXDOMAIN in the language of BIND, the dominant DNS server software).[6] The user's application could then respond to the NXDOMAIN message as it saw fit. Some web browsers return a simple error message that the web page in question cannot be found. Microsoft's Internet Explorer directs the user to a page within <search.microsoft.com> that offers the user the opportunity to use the

---

5. See Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge: MIT Press, 2002); A. Michael Froomkin, "Wrong Turn in Cyberspace: Using ICANN to Route Around the APA & the Constitution" (2000) 50 Duke L.J. 17, <http://www.law.duke.edu/shell/cite.pl?50+Duke+L.+J.+17> [Froomkin, "Wrong Turn"]; Jonathan Weinberg, "ICANN and the Problem of Legitimacy" (2000) 50 Duke L.J. 187, <http://www.law.duke.edu/shell/cite.pl?50+Duke+L.+J.+187> [Weinberg].

6. The official DNS protocol specification, RFC 1035, defines this response as RCODE 3 ("name error"). See Paul Mockapetris, Request for Comments: 1035, "Domain Names—Implementation and Specification," *Internet Engineering Task Force* (24 November 1987), <http://www.rfc-editor.org/rfc/rfc1035.txt> ["RFC 1035"]; "Message from Security and Stability Advisory Committee to ICANN Board" *ICANN* (22 September 2003), <http://www.icann.org/correspondence/secsac-to-board-22sep03.htm> ["SECSAC Recommendations"]; "Internet Architecture Board Commentary: Architectural Concerns on the Use of DNS Wildcards" *IAB* (19 September 2003), <http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html> ["IAB Commentary"]; see also Mark Andrews, Request for Comments: 2038, "Negative Caching of DNS Queries" *Internet Engineering Task Force* (17 March 1998), <http://www.rfc-editor.org/rfc/rfc2308.txt> (describing NSDOMAIN as an alternate expression).

   For exceptions, see *infra* notes 88–92 and accompanying text. In addition, Neulevel, which operates the BIZ domain, ran a test of a Site Finder-like service for several days in May 2003. See email from Karl Auerbach to the bwg+ mailing list (16 September 2003) (on file with author).

MSN Search service. Email software declines to send the mail, instead returning a "Host unknown" error message.

For the past twelve years, the registry databases for the two largest top-level domains—COM and NET—have been operated by VeriSign (or its predecessor in interest, Network Solutions, Inc.).[7] On September 15, 2003, largely without warning,[8] VeriSign instituted a new behaviour for those two registries, which between them include most of the domain name space.[9] Under the new behaviour, all queries for nonexistent domain names resolved to a new set of servers operated by VeriSign instead of returning "no such address" responses.[10] When one of those servers received a request for a web page, it sent the user to a VeriSign-generated page, in English, suggesting other similar domain names that the user might like to try and offering a series of category links for the user to follow. The user's clicking on those links generated new revenue for VeriSign via pay-per-click search functionality operated by a third-party service.[11] When the VeriSign redirection server received email, it bounced it. When the server received packets relating to any other internet application, it performed a TCP reset or dropped the packets, so that the user appeared to have experienced an unexplained connection failure.[12] VeriSign called this new behavior its "Site Finder service," and described the change as an improvement intended to generate more helpful error pages for Web surfers.

Reaction by the internet technical community to Site Finder was swift and vitriolic. The news broke on the influential NANOG (North American Network Operators Group) mailing list in a series of messages with the subject line "*What*

---

7. VeriSign and Network Solutions also operated the ORG domain until December 31, 2002, and the EDU domain until 2001. From 1991 to 1993, Network Solutions operated the four registries pursuant to a subcontract from Government Services, Inc.; beginning in 1993, it performed that function pursuant to a cooperative agreement with the U.S. National Science Foundation. See Weinberg, *supra* note 5 at 198–99; *PGMedia, Inc. v. Network Solutions, Inc.*, 51 F.Supp. 2d 389 at 393 (S.D.N.Y. 1999), *aff'd*, 202 F.3d 573 (2d Cir. 2000). In 1998, the U.S. Department of Commerce replaced the National Science Foundation as the government entity administering the cooperative agreement. Weinberg, *supra* note 5 at 211, n. 126. In 2000, VeriSign purchased Network Solutions; the deal was valued at $21 billion. See Melanie Austria Farmer, "VeriSign Buys Network Solutions in $21 Billion Deal" *CNET News.Com* (7 March 2000), <http://news.com.com/2100-1023-237656.html>.

8. There had been scattered press reports leaking news of the change within the previous ten days. See "SECSAC Recommendations," *supra* note 6.

9. About 60% of all unique internet hosts worldwide are registered under the COM and NET domains. "Distribution by Top-Level Domain Name by Name" *Internet Software Consortium* (January 2003), <http://www.isc.org/ops/ds/reports/2003-01/dist-byname.html> ["Distribution by Top-Level Domain"]. The same source suggests that COM and NET include more than 70% of all second-level domain names, but that measure doesn't take into account the fact that in some country-code name spaces, third-level domains play the same functional role as second-level domains in COM. "The Daily Domain Counts of Domains Worldwide" *Domain Worldwide* (13 November 2003), <http://www.domainworldwide.com/> addresses this by treating domains under .CO.UK, and similar country-code zones, as second-level domains for the purpose of the count. By that count, COM and NET include 54% of all second-level domains.

10. See "VeriSign's Site Finder Implementation" *VeriSign, Inc.* (27 August 2003), <http://www.verisign.com/resources/gd/Site Finder/implementation.pdf>. This document was released to the public on September 15, 2003. See posting by Dave Farber, dave@farber.net, to ip@v2.listbox.com "[IP] All your Misspelling Are Belong to Us" *Interesting-People* (16 September 2003), <http://lists.elistx.com/archives/interesting-people/200309/msg00141.html>.

11. See posting by Dave Farber, dave@farber.net, to ip@v2.listbox.com, "[IP} Overture Service and VeriSign Now Owns Your Use of .COM and .NET?" *Interesting-People* (17 September 2003), <http://lists.elistx.com/archives/interesting-people/200309/msg00162.html>. The service, Overture, Inc., accepts bids from website owners for placement of links to their sites in its search page results. Several other web search services, including MSN Search, are also Overture customers. (*Ibid*).

12. See "IAB Commentary," *supra* note 6.

**are* they smoking?"*[13] Typical comments in that discussion described VeriSign's move as "technically and business slimy,"[14] or a "horribly inappropriate scam,"[15] or asked, "VeriSign: WHO DO YOU THINK YOU ARE?"[16] Participants traded ideas for blocking or ameliorating the change. The reaction from bigger DNS players was to the same effect, although more politely worded.[17]

Two days later, on September 17, came a mailing from the Internet Software Consortium (ISC). ISC maintains the BIND software that performs the domain name lookups on the vast majority of DNS servers. In response to what ISC described as "high demand from our users," it released a patch to BIND that, at an internet service provider's election, would cause it to ignore the synthesized records that VeriSign used to direct queries for nonexistent domains to the Site Finder server.[18] After an internet service provider applied the patch, its DNS resolver could once again return an NXDOMAIN response when confronted with a query for a nonexistent domain. This remarkably quick fix generated its own set of concerns; operators of the NAME top-level domain complained that users were configuring the patch injudiciously and blocking email to some users of that domain.[19] ISC released two updated versions and incorporated the patch into the regular BIND release.[20]

On September 18, the company operating the Netster SmartBrowse program, which had supplied a Site Finder-like search page to users mistyping domain names, sued VeriSign. It claimed that VeriSign's implementation of the service amounted to an abuse of monopoly power, violating the *Sherman Act*[21] and federal and state unfair competition law.[22]

On September 19, the Internet Architecture Board (IAB) issued a lengthy statement.[23] The IAB sits atop the Internet Engineering Task Force (IETF), super-

---

13. See North American Network Operators 0309 By Thread (September 2003), <http://www.irbs.net/internet/nanog/0309/>.
14. George William Herbert, "Re: What *are* they smoking?" (15 September 2003), <http://www.irbs.net/internet/nanog/0309/0392.html>.
15. Richard A. Steenbergen, "Re: What *are* they smoking?" (15 September 2003), <http://www.irbs.net/internet/nanog/0309/0394.html>.
16. Daniel Roesen, "Re: What *are* they smoking?" (15 September 2003), <http://www.irbs.net/internet/nanog/0309/0407.html>.
17. See *e.g.* Letter from Cigref to VeriSign (19 September 2003), <http://www.icann.org/correspondence/cigref-to-verisign-en-19sep03.htm> (characterizing Site Finder implementation as astonishing and regrettable, raising issues of security, ethics and legality); Letter from Register.com to VeriSign (19 September 2003), <http://www.icann.org/correspondence/registercom-to-verisign-19sep03.pdf> (urging that Site Finder is deceptive, illegal, and an abuse of VeriSign's monopoly power); Letter from Public Interest Registry to Paul Twomey (22 September 2003), <http://www.icann.org/correspondence/maher-to-twomey-22sep03.pdf> (urging that Site Finder "introduces significant problems to critical Internet infrastructure").
18. See "ISC BIND 'delegation-only' Feature" *Internet Software Consortium* (23 October 2003), <http://www.isc.org/products/BIND/delegation-only.html> ["ISC BIND"]. For some technical explanation, see posting by Tanner Lovelace, "[TriLUG] Delegation only Patch for Bind" (17 September 2003), <http://www.trilug.org/pipermail/trilug/Week-of-Mon-20030915/020275.html>.
19. Letter from Geir Rasmussen, CEO, Global Name Registry, to Stephen Crocker, Chair, ICANN Security and Stability Advisory Committee (13 October 2003), <http://www.icann.org/correspondence/gnr-to-secsac-13oct03.pdf>.
20. See "ISC BIND," *supra* note 18.
21. 15 U.S.C.S. § 3 (2002).
22. Complaint and Demand for Preliminary Injunction, *Popular Enterprises, LLC v. Verisign, Inc.* (M.D. Fla. filed 18 September 2003), <http://search.netster.com/about/lawsuit.asp>.
23. "IAB Commentary," *supra* note 6.

vising its standards-development process.[24] It is the closest thing to a governing body the internet technical community has, but its powers are limited; it cannot force any company to comply with the IETF's consensus-based standards.[25] The IAB noted that in order to make Site Finder possible, VeriSign had inserted what are known as wildcard records in the COM and NET zones. While this use of wildcards did not technically violate IETF standards, the IAB continued, it violated assumptions that were inherent to internet architecture.[26] The result "was disastrous for the users."[27] A registry should not use wildcards in registry zones, as VeriSign was doing, unless it could carry the burden of showing that its action would not "pose a threat to stable operation of the DNS or predictable behaviour for applications and users."[28] The IAB recommended that VeriSign remove its wildcards "at the earliest opportunity."[29]

The same day, ICANN entered the fray. ICANN had been created in 1998 as a "new, not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system."[30] VeriSign administers the COM and NET registries pursuant to a set of contracts with ICANN.[31] Though its legitimacy has been challenged, its power at least over the creation of new top-level domains in the legacy root is clear. ICANN released an advisory explaining that it had requested advice on Site Finder from the IAB and from its own Security and Stability Advisory Committee (SECSAC). SECSAC is a group of two dozen internet engineers collected by ICANN as an advisory committee.[32] Its only function within the ICANN structure is to issue non-binding advisories and recommendations,[33] but the fact that its members are held in high regard in the internet technical community gives its recommendations weight. ICANN called upon VeriSign to suspend its service voluntarily until those reviews were completed.[34]

VeriSign declined. In a letter, it answered that it had deployed Site Finder "after many months of testing and analysis and in compliance with all

---

24. See "Internet Architecture Board Overview" *IAB*, <http://www.iab.org/about/overview.html>.
25. See Brian Carpenter, "What Does the IAB Do, Anyway?" *IAB*, adapted from an article appearing in (1996) 10:2 ConneXions, <http://www.iab.org/about/description.html>. See A. Michael Froomkin, "Habermas@discourse.net: Toward a Critical Theory of Cyberspace" (2003) 116 Harv. L. Rev. 749 at 783–93; Joseph Reagle, "Why the Internet is Good: Community Governance that Works Well" (undated) Berkman Center for Internet and Society, <http://cyber.law.harvard.edu/people/reagle/regulation-19990326.html> [Reagle]; Weinberg, *supra* note 5 at 250–255.
26. "IAB Commentary," *supra* note 6. Though the document never mentions VeriSign by name, its references are clear.
27. *Ibid.*
28. *Ibid.*
29. *Ibid.*
30. U.S., Department of Commerce, *Management of Internet Names and Addresses* (S. Doc. No. 980212036-8146-02) (Washington, D.C.: 1998), <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>. The twisting process that led to ICANN's creation has been well-described elsewhere. See sources cited in *supra* note 5.
31. See ".com Registry Agreement" *ICANN* (25 May 2001), <http://www.icann.org/tlds/agreements/verisign/registry-agmt-com-25may01.htm > [".com Registry Agreement"].
32. "Security and Stability Advisory Committee" *ICANN* (undated), <http://www.icann.org/committees/security/>.
33. See "Security Committee Charter" *ICANN* (14 March 2002), <http://www.icann.org/committees/security/charter-14mar02.htm>.
34. "Advisory Concerning VeriSign's Deployment of DNS Wildcard Service" *ICANN* (19 September 2003), <http://www.icann.org/announcements/advisory-19sep03.htm> ["Advisory"].

applicable technical standards."[35] "Users," it wrote, "were benefiting from the improved web navigation offered by Site Finder."[36] VeriSign was certainly interested in the operational impact of its implementation, and had asked a technical review panel to look at that issue. It continued:

> As to your call for us to suspend the service, I would respectfully suggest that it would be premature to decide on any course of action until we first have had an opportunity to collect and review the available data. After completing an assessment of any operational impact of our wildcard implementation, we will take any appropriate steps necessary.[37]

On September 22, SECSAC issued a statement calling on VeriSign to voluntarily suspend Site Finder. Site Finder, SECSAC said, had "considerably weakened the stability of the Internet" and "introduced ambiguous and inaccurate responses in the DNS."[38] VeriSign again declined. Noting that SECSAC had scheduled a public meeting for three weeks later to gather information, VeriSign charged that SECSAC's initial conclusions were uninformed and premature, and that the committee had initiated a biased and unfair process to gather data *post hoc*. SECSAC's actions to date had so poisoned the well, it continued, that its public hearing could not possibly be conducted with neutrality, objectivity, integrity and fairness.[39]

In the meantime, two more lawsuits were filed. Go Daddy Software, a domain-name registrar, sued VeriSign raising *Sherman Act* monopolization and unfair competition claims.[40] Internet litigator (and gadfly) Ira Rothken filed a lawsuit raising a slew of causes of action on behalf of two putative nationwide plaintiff classes.[41] The first was all persons or entities who engage in internet commerce and who use programs or systems that rely on domain name error messages. The second was all persons or entities "who have been, or are likely to be," redirected to the Site Finder site.[42] Since there are said to be in excess of 185 million people in the United States using internet-based applications,[43] and the vast majority of that group would be class members, these would be very large plaintiff classes indeed.

On October 3, ICANN altered the state of play by issuing a "formal demand" to VeriSign "to return the operation of the .com and .net domains to their state before the 15 September changes, pending further technical, opera-

---

35. Letter from Russell Lewis, Exec. VP, VeriSign, to Paul Twomey, CEO, *ICANN* (21 September 2003), <http://www.icann.org/correspondence/lewis-to-twomey-21sep03.htm>.
36. *Ibid.*
37. *Ibid.*
38. "SECSAC Recommendations," *supra* note 6.
39. Letter from James Ulam, General Counsel, VeriSign, to John Jeffrey, General Counsel, ICANN (3 October 2003), <http://www.icann.org/correspondence/verisign-to-icann-03oct03.pdf>.
40. See Verified Complaint and Application for Preliminary Injunction, *GoDaddy Software, Inc. v. VeriSign, Inc.* (D. Ariz. 2003), available at <https://www.godaddy.com/gdshop/pressreleases/complaint.pdf?isc=&se=%2B&from%5Fapp=>.
41. See Class Action Complaint for Equitable and Injunctive Relief, *Syncalot, Inc. v. VeriSign, Inc.* (N.D. Cal. 2003) at 5, available at <http://www.techfirm.com/v-complaint.pdf>.
42. *Ibid.*
43. See Nielsen/NetRatings, <http://www.netratings.com/news.jsp?section=dat_to&country=us> (visited 15 November 2003).

tional and legal evaluation."[44] The Site Finder implementation, according to ICANN's letter, "had a substantial adverse effect on the core operation of the DNS, on the stability of the Internet, and on the relevant domains."[45] Perhaps more to the point, it was inconsistent with VeriSign's contractual obligations to ICANN under the .com and .net registry agreements. The letter concluded: "Failure to comply with this demand by [6 pm PDT the following day] will leave ICANN with no choice but to seek promptly to enforce VeriSign's contractual obligations."[46]

VeriSign complied grudgingly. ICANN's action, it complained, was groundless, factually unsupported, anti-competitive, and itself a violation of the registry agreements. VeriSign threatened to hold ICANN accountable in damages for that improper interference with its contractual and other business relationships. But it felt, in light of ICANN's position, that it had "no alternative but to temporarily suspend the service."[47]

This was not the end of the story from either side's perspective. VeriSign has indicated that it plans to reactivate Site Finder later on, after making technical improvements.[48] It has said nothing about asking ICANN for permission first.

ICANN staff, for their part, are seeking to institute a "timely, transparent and predictable process" for prior ICANN review of all changes instituted by generic[49] top-level domain registries that, "because of their architecture or operation, could affect the operational stability, reliability, security or global interoperability of the DNS, that registry, or the Internet."[50] As this article goes to press, ICANN has released an issues report setting out the rationale for the change.[51] Under normal circumstances, the next step in the policy development process would be for ICANN's Generic Names Supporting Organization Council[52] to form a representative task force to consider the issue. The report, however, urges the Council to skip that step so that ICANN staff can immediately generate a proposal, for adoption by the Council, on the basis of comments submitted to staff

---

44. Letter from Paul Twomey, CEO, ICANN, to Russell Lewis, Exec. VP, VeriSign (3 October 2003), <http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm>.
45. *Ibid.*
46. *Ibid.*
47. Letter from Russell Lewis, Exec. VP. VeriSign, to Paul Twomey, CEO, ICANN (3 October 2003), <http://www.icann.org/correspondence/VeriSign-to-twomey-03oct03.pdf>.
48. See Dan Gillmor, "VeriSign's Arrogant Excuses for Tinkering with the Net" (6 October 2003), <http://weblog.siliconvalley.com/column/dangillmor/archives/001394.shtml>; see also McCullagh, *supra* note 1.
49. Domain-name lingo speaks of "generic" top-level domains, such as COM and NET, to distinguish them from "country-code" top-level domains, such as US and FR.
50. "Staff Manager's Issue Report," *supra* note 3.
51. *Ibid.*
52. "[T]he Generic Names Supporting Organization (GNSO)…shall be responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains." ICANN Bylaws, art. X, § 1, <http://www.icann.org/general/bylaws.htm>. The GNSO Council is responsible for managing the policy development process of the GNSO. (*ibid.* art. X, § 2).

by the various "constituencies"[53] and the public.[54] ICANN's CEO has indicated that the entire process should be completed by January 15, 2004.[55] This is, almost surely, wildly optimistic.[56]

*

2.

SO WHAT SHOULD WE THINK of Site Finder from a technical perspective? Did it "considerably weaken[] the stability of the Internet,"[57] as the SECSAC concluded, or was it a "valuable service to the Internet community,"[58] fully standards-compliant and raising no significant problems, as VeriSign insisted? In order to answer that question, I will start by reviewing some of the objections made by Site Finder critics.

An initial set of objections came from the operators of spam filters. One technique used by some software to identify spam is to check whether the purported sending domain actually exists; if the check returns NXDOMAIN, then the message is plainly bogus. Once Site Finder was in place, though, that technique was useless, since the VeriSign registries no longer returned NXDOMAIN error messages. Rather, any alphanumeric string in front of ".com" or ".net" would generate a NOERROR registry response, incorporating a pointer to the Site Finder site, that the unsuspecting spam filter would understand as signifying a live, functioning, domain.[59]

Nor were spam filters the only programs for which Site Finder created problems; other programs, such as link checkers,[60] were confused as well. More generally, Site Finder caused problems (or had the potential to cause problems) for any internet application relying on HTTP (the World Wide Web protocol) in which the user was not a human being sitting in front of a computer displaying a

---

53. The ICANN structure grants a seat at the decision-making table to six constituencies, each "recognized as representative of a specific and significant group of stakeholders": gTLD registries, registrars, ISPs and connectivity providers, "commercial and business users," noncommercial organizations, and trademark owners. See ICANN Bylaws, art. X, s. 5.1, <http://www.icann.org/general/bylaws.htm#X>; Weinberg, *supra* note 5 at 238–42.

54. For the relevant bylaws provisions, see ICANN Bylaws, Annex A, <http://www.icann.org/general/bylaws.htm#AnnexA>. The Chair of the GNSO Council has responded, as this article goes to press, by suggesting that the Council dispense with the task force but instead constitute itself as a committee of the whole to work with ICANN staff so that the initial staff report comes as close as possible to reflecting a consensus of the Council. See Bruce Tonkin, "[Council] Policy Development Process Without a Task Force" (21 November 2003), *ICANN/GNSO GNSO Email List Archives* <http://www.gnso.icann.org/mailing-lists/archives/council/msg00308.html>.

55. Letter from Paul Twomey, CEO, ICANN, to Bruce Tonkin, Chair, ICANN Generic Names Supporting Organization Council (20 October 2003), <http://www.icann.org/correspondence/twomey-to-tonkin-20oct03.pdf>.

56. For one thing, the GNSO Council will not even decide its procedural vehicle, see *supra* note 54, until the beginning of December 2003, and the draft terms of reference document that is on the table for adoption at that meeting reflects some substantive viewpoints decidedly contrary to those in the issue report. GNSO Council Teleconference Agenda (2 December 2003), <http://www.gnso.icann.org/meetings/agenda-02dec03.shtml>; see *infra* notes 154–156 and accompanying text.

57. "SECSAC Recommendations," *supra* note 6.

58. *Supra* note 47.

59. See posting by Dave Farber, dave@farber.net, to ip@v2.listbox.com "[IP] ICANN—Formal Complaint re VeriSign Good Summary of the Problems" (18 September 2003), available at *Interesting-People,* <http://lists.elistx.com/archives/interesting-people/200309/msg00180.html>.

60. See "Link Checking Routine," *Andilinks* <http://www.andilinks.com/linkckg.htm> (visited 2 November 2003).

web browser. Thus, for example, SOAP—a protocol for exchanging structured information between applications over the web—reacted badly to Site Finder.[61] SOAP, like a variety of other document-based interactions on the web, operates on the machine-to-machine level, and the Site Finder page was not set up to communicate with machines.

Other observers complained about the way Site Finder handled email. Previously, email sent to a nonexistent address generated an immediate error message, without complications or undue bandwidth consumption. Given Site Finder, a user's misaddressed email had to travel to the VeriSign bounce server and back, thus increasing the load on the user's ISP.[62] The unexpected Site Finder response caused a variety of email programs to provide misleading or delayed error messages when they were confronted with mistyped addresses or misconfigured.[63]

Further, any problem with the machines VeriSign was running to catch and return email sent to nonexistent addresses meant a long delay in getting an error message to the user; typographical errors that, pre-Site Finder, would have been caught immediately might go unnoticed for several days, or perhaps indefinitely.[64] Indeed, in a few cases, mail sent to a valid address might not get through. If a user's principal mail server had an erroneous or expired MX record, or if a transient network error made it seem that way, then Site Finder would bounce the mail rather than allowing it to flow through to even a well-configured backup mail server.[65] Alternatively, if a user's principal mail server were down for maintenance and the backup server was under an expired domain, then Site Finder would bounce the mail rather than allowing it to be queued for delivery to the principal mail server, as standard protocols contemplated.[66]

Other objections went more nearly to the core of the Site Finder service. The point of the enterprise, according to VeriSign, was to provide users with something more helpful than an opaque error page when they accidentally typed

---

61. See posting by Dave Farber, dave@farber.net, to ip@v2.listbox.com "[IP] Site Finder Confuses SOAP Implementations" (29 September 2003), available at *Interesting-People*, <http://lists.elistx.com/archives/interesting-people/200309/msg00275.html>. See generally World Wide Web Consortium, SOAP Version 1.2 Part 1: Messaging Framework (24 June 2003), <http://www.w3.org/TR/soap12-part1/> (describing SOAP).

62. See "IAB Commentary," *supra* note 6.

63. See Richard M. Smith, "Why Site Finder is Breaking MS Outlook & Windows Networking Utilities" *CircleID* (21 September 2003), <http://www.circleid.com/article/273_0_1_0_C/>; "IAB Commentary," *supra* note 6.

64. See "IAB Commentary," *supra* note 6.

65. See Chuck Liggett, "RE: [ga] Some Wild-Card Questions" (17 September 2003), *ICANN/GNSO GNSO Email List Archives*, <http://gnso.icann.org/mailing-lists/archives/ga/msg00362.html>; Posting by Dave Farber, dave@farber.net, to ip@v2.listbox.com "[IP] This is How Badly Broken Site Finder Is" (17 September 2003) available at *Interesting-People*, <http://lists.elistx.com/archives/interesting-people/200309/msg00171.html>; Lydia Leong, "Take Immediate Action Against VeriSign Site Finder" *Gartner.com* (18 September 2003), <http://www.gartner.com/DisplayDocument?doc_cd=117392>.

66. See email from Paul Vixie, "Re: VeriSign SMTP Reject Server Updated" (20 September 2003), <http://www.irbs.net/internet/nanog/0309/1007.html>; Email from Thomas Roessler, "Another Site Finder issue" (17 September 2003), <http://does-not-exist.org/mail-archives/alac/msg00098.html>. Site Finder also raised privacy and security issues since mail intended for recipients other than VeriSign was now hitting the Site Finder server, a place its senders had not intended it to go. See "IAB Commentary," *supra* note 6 where the IAB suggested that hackers attacking and taking control over Site Finder's mail handling capabilities could gain access to large amounts of misaddressed mail. At least at the outset, the Site Finder mail server was configured so as to be aware of both the sender and putative recipient of the misaddressed mail routed to it. See Jason Garman, "Site Finder: The Technical, Legal & Privacy Concerns" *CircleID* (18 October 2003), http://www.circleid.com/article/267_0_1_0_C/#technical>. VeriSign later moved to a better-configured setup.

an address for a nonexistent domain. Yet there was already plenty of software out there that performed that function. Before Site Finder, after all, a user's machine could run a variety of programs to interpret an NXDOMAIN message in the context of a particular application running on the user's desktop. A person who wanted a Site Finder-like response from her web browser could get it by choosing Internet Explorer as her web browser; the copy of Internet Explorer running on her machine, when receiving the NXDOMAIN message, would display an MSN Search page. That response, taking place within the browser on her own machine, would not affect any other user. A person who wanted different functionality could run different programs, such as Netscape with the Google Toolbar. A user in a non-English-speaking country, who wanted Site Finder-like functionality in his native language, incorporating local conventions and directories, could run a browser or plug-in that provided it. None of these programs worked after Site Finder. Similarly, Site Finder eliminated other forms of custom error handling, like those found in browsers designed for visually-impaired users, or in browsers in handheld or other nonstandard devices.[67] Users all over the world, instead of getting NXDOMAIN messages to be interpreted by the programs the users saw fit to install on their machines, were now getting a one-size-fits-all, English-language search page from VeriSign.[68]

Moreover, with the one-size-fits-all web page came other problems associated with a centralized, single point of failure. Unless VeriSign robustly provisioned the Site Finder servers, those servers could be overwhelmed (as indeed they were in Site Finder's early days). In that situation, users would get neither an error message nor the Site Finder page, but simply an "attempting to connect..." message followed by a long wait.[69] There were also privacy concerns. With amazing insouciance, VeriSign had set up the Site Finder page to set a cookie on the user's hard drive, and to report (via a web bug) such information as the mistyped address, the page the user had been on previously, the user's browser type, etc.[70] Indeed, if a user filled out a web form that the server submitted to an action URL with a misspelled or expired domain name, then the Site Finder web bug would transmit the

---

67. Statement of David Schairer, Vice President, XO Communications, at the SECSAC Meeting: Real-Time Captioning, *ICANN* (7 October 2003), <http://SECSAC.icann.org/captioning-07oct03.htm> [SECSAC Meeting].

68. *Ibid.* That page, moreover, used more bandwidth than the error message would have. The difference may have been significant in countries where user connections are slow, and charges for internet service are volume-based.

69. See *ibid.*; Russell Smith, "[ga] FW: VeriSign's Site Finder Service" (17 September 2003), *ICANN/GNSO GNSO Email List Archives* <http://gnso.icann.org/mailing-lists/archives/ga/msg00358.html>; see also "IAB Commentary," *supra* note 6.

70. See Richard M. Smith, "Bug Reveals the Snooper in VeriSign's Site Finder" *CircleID* (17 September 2003), <http://www.circleid.com/article/260_0_1_0_C/>; Security Focus, "VeriSign's Site Finder Finds Privacy Hullabaloo" *The Register* (19 September 2003), <http://www.theregister.co.uk/content/6/32926.html>. A VeriSign spokesperson, it should be noted, took a firm position that "[w]e do not log, and do not have any plans to log, any data sent to Site Finder." Paul Roberts, "VeriSign Accused of Privacy Violation" *PCWORLD* (19 September 2003), <http://www.pcworld.com/news/article/0,aid,112572,00.asp>. Still, as one observer responded, "there *is* that web bug on their web page that *is* collecting lots of information….So I wonder just who did put that web bug onto their web pages? Elves?" Comment by Karl Auerbach, "So Who Put the Web Bug There?" *ICANNWATCH* (21 September 2003), <http://www.icannwatch.org/article.pl?sid=03/09/20/160208>.

information the user had filled in, including email addresses or passwords.[71]

Finally, there were problems associated with the fact that Site Finder simply dropped any packets associated with protocols other than HTTP (the web) and SMTP (email). Applications using those protocols did not receive the error messages they were expecting in connection with incorrect names; instead, they simply reported connection errors. Depending on how an application was written, it could continue trying to connect for days or even weeks, rather than recognizing the problem immediately.[72]

None of these problems were, by themselves, fatal. Most of them, one way or another, could be avoided or ameliorated. Some of them were simply the result of poor planning on VeriSign's part. Presumably because it understood the overwhelming negative reactions it would have received had it discussed the Site Finder plan with the internet technical community in advance of implementation, VeriSign had worked out its engineering plans in secret and then sprung them on the community as a *fait accompli*.[73] To the extent that we view VeriSign's deployment of registry-zone wildcards as the equivalent of a change in underlying DNS protocols, that secrecy was plainly inappropriate; long-standing internet practice is that such changes take place only after extensive discussion within the internet technical community, so that bugs can be worked out and a rough consensus can emerge for, or against, the change.[74] VeriSign and its supporters have urged that no such discussion was necessary in this case because Site Finder was simply an implementation of existing protocols.[75] This position is problematic given that Site Finder affected the operational stability of a wide range of existing applications and services across organizational boundaries. One thing, however, is clear: VeriSign's secrecy was reflected in the relatively poor quality of its implementation. Its initial email server, for example, was buggy and not standards-compliant, and VeriSign hurriedly replaced it.[76] VeriSign could have ameliorated other problems had it had the benefit of criticism in advance. For example, it could have used language tags in HTTP queries to support responses in at least some local languages other than English. Because HTTP language tags do not always match the user's location, this would have been a second-best

---

71. See Richard M. Smith, "Site Finder Is Leaking Data" *CircleID* (23 September 2003), <http://www.circleid.com/article/286_0_1_0_C/>.

72. See "IAB Commentary," *supra* note 6.

73. VeriSign has indicated that it did, in advance of September 15, work privately with a variety of outside companies to test the service and identify problems in connection with specific applications. It suggested that the reason it did not discuss its plans publicly was to avoid "getting so specific that we expose things to our competitors." Response of Chuck Gomes, SECSAC Meeting, *supra* note 67; see also *supra* note 1, noting that VeriSign confidentially briefed about 35 outside companies, and assembled a technical review panel, before Site Finder's launch.

74. See *e.g.* Scott Bradner, Request for Comments: 2026, "The Internet Standards Process—Revision 3" *Internet Engineering Task Force* (October 1996), <http://www.ietf.org/rfc/rfc2026.txt>.

75. See Keith Teare, "VeriSign's Site Finder" (17 October 2003), <http://weblog.teare.com/comments.php?id=P172_0_1_0>.

76. See David Schairer, Presentation at SECSAC Meeting, "Consequences I: What Was Affected" *ICANN* (7 October 2003), <http://www.icann.org/presentations/shairer-secsac-dc-07oct03.ppt>; Matt Larson, "VeriSign SMTP reject server updated" (20 September 2003), <http://www.irbs.net/internet/nanog/0309/0992.html>. VeriSign has now indicated that it believes that a different solution—"a wildcard MX record pointing to a nonexistent target"—would be a better solution still. Comment of Matt Larson, SECSAC Meeting, *supra* note 67.

solution,[77] but still far better than VeriSign's initial approach.[78]

The other way to ameliorate Site Finder problems derived from the overall nature of many of those problems. A wide range of internet application programs, ranging from spam filters to email clients to XML-based applications and more, were written against a set of background assumptions about how the DNS would behave when confronted with a string that did not correspond to a registered domain name. After Site Finder, those assumptions no longer held true. Consequently, the programs did not operate as their authors had intended. As the IAB put it, "[t]he small but fundamental way in which [wildcards] change the record lookup rules has a nasty way of violating implicit (or, sometimes, explicit) assumptions in deployed DNS-using software."[79] The universe of software that depends on "no such name" responses, for which those assumptions are material, "turns out to be quite large."[80]

This suggests that the authors of internet applications boggled by Site Finder could address those problems by modifying them to incorporate a new set of assumptions. Spam filter writers, for example, could modify them to recognize responses from the Site Finder IP address.[81] Doing so would be an unwelcome burden for application writers, but for the most part it would not be beyond their powers. As the IAB put it, "a significant component of some of the listed problems was not precisely the wildcard-induced behavior per se so much as it was the abrupt change in the behaviour of a long established infrastructure mechanism."[82] Part of VeriSign's published defences of Site Finder, thus, suggested that the onus should be on software developers to accommodate the changes that Site Finder made.[83]

This brings us to the key question: How bad *was* Site Finder? Plainly, it created a variety of problems, but were the difficulties it presented merely those of a brief, transitional period of adjustment and upgrade, or did they reflect a fundamental challenge to the existing internet architecture? In the end, my vote is for the latter. Adjusting to Site Finder *would* have presented difficulties of transition and adjustment; one expert described it as necessitating "a reevaluation of old code, similar in concept, much smaller in scope, to the Y2K preparations."[84] But Site Finder's problem is more fundamental.

---

77. See "IAB Commentary," *supra* note 6.
78. VeriSign has indicated that it plans to introduce local-language capability for German, Japanese, Spanish, French, and Chinese users. VeriSign's Response to IAB Commentary (6 October 2003), <http://www.icann.org/correspondence/verisign-response-iab-06oct03.pdf>.
79. "IAB Commentary," *supra* note 6.
80. *Ibid.*
81. *Ibid.*
82. *Ibid.*
83. See Letter from Russell S. Lewis, Exec. VP, VeriSign to Paul Twomey, CEO, ICANN (6 October 2003), available at <http://icann.org/correspondence/VeriSign-response-iab-06oct03.pdf>, contending that "[a]nti-spam software…can be easily updated to operate in the presence of wildcard entries in the .com and .net zones."; "Application Developer's Guide to DNS Wildcards" *VeriSign* (7 August 2003), cited in Jonathan Zittrain & Benjamin Edelman, "Index of Concerns as to VeriSign Site Finder" (7 October 2003), <http://cyber.law.harvard.edu/tlds/Site Finder/concerns.html> ["Index of Concerns"], stating that for existing applications that do not contemplate the effects of wildcard entries, "application developers should consider taking appropriate corrective actions."
84. Statement of David Shairer, SECSAC Meeting, *supra* note 67.

Part of the basic design philosophy of the internet has been that innovation takes place at the edges. The Net is what David Isenberg famously called a "stupid network;"[85] its proper function is nothing other than to deliver bits from point A to point B, without their encountering especially intelligent control mechanisms along the way.[86] Where the network does nothing more than move bits between the end points, innovation can take place on the edges, without the permission of the system operator (or the IETF), via the applications run on the endpoint computers. As Steve Bellovin put it, "you want to make sure that the center does as little as possible so that it does not prevent the end from doing the right thing" in any given context.[87] The fact that the Net enables innovation at the edges is what has made possible the unrestrained development and dissemination of every new internet service, whether it be the web, IP telephony, or peer-to-peer file sharing. The folks seeking to implement those services did not need to involve the IETF or network operators. They could implement new services simply by running applications on client machines, relying on the network's lower protocol levels to carry packets from one client to the next.

The key problem with Site Finder is that it took the function of interpreting "no such domain" messages from client software, and built it into the infrastructure of the domain name system itself. It thus substituted monopoly for competition; it prevented the user from invoking any other service to deal with mistyped names no matter how far superior or better suited to particular user needs. VeriSign representatives have stressed that the user interface should display an intelligent user-friendly response, rather than an opaque error message, when users seek a nonexistent internet resource. That makes sense. The question, though, is from whom users should get that response. Building that functionality into the domain-name infrastructure (where it fits badly, since the DNS was built to be a deterministic lookup engine, not a generator of fuzzy, pay-per-click "maybe you meant…" pages) cuts against basic principles of internet architecture and serves users badly.

To be sure, one very small generic top-level domain (MUSEUM) had earlier implemented wildcards without obvious ill effect, as had eleven country-code top-level domains.[88] In very small zones, wildcards can be less problematic. The web page returned by MUSEUM in response to an HTTP request for a non-existent name, for example, refers the user to a list of *every* second-level name in the MUSEUM domain; that's actually helpful, and there are advantages to putting that functionality in the hands of the entity that keeps the zone file, but it works

---

85. See David Isenberg, "Rise of the Stupid Network" (August 1997) Computer Telephony 16, available at <http://www.hyperorg.com/misc/stupidnet.html>.

86. For a more sophisticated explication of this thesis, and an explanation of why it is usually not cost-effective to build intelligence into the network, see Jerome H. Saltzer, David P. Reed & David D. Clark, "End-to-end Arguments in System Design" (1984) 2 ACM Transactions on Computer Systems 277.

87. Statement of Steven Bellovin, AT&T Labs-Research, SECSAC Meeting, *supra* note 67.

88. See Chip Salzenberg, "VeriSign is Not Alone" (17 September 2003), *Google Newsgroup news.admin.net-abuse.email*, <http://www.google.com/groups?selm=ag%259b.389403%24Os1.2925096%40news.easynews.com>; Museum Domain Management Association, *Statement Concerning Wildcard A Records in Top-Level Domains* (6 October 2003), <http://musedoma.museum/policy/wildcard/>.

only because the list includes fewer than 650 names.[89] Some of the ccTLDs implementing wildcards are significantly larger; they include the DNS's 59th and 61st largest top-level domains, PH (Philippines) and CC (Cocos Islands, but run by a VeriSign subsidiary and marketed worldwide).[90] Those two registries appear to have implemented wildcards for marketing purposes; an HTTP request for an unassigned name generates a page advertising that the page is available for sale.[91] This isn't great, but the wildcards are still relatively unproblematic for two reasons. First, these domains are still relatively small. Second, the country-code domain name community as a whole faces larger challenges; the size and sophistication of ccTLD registries vary tremendously, and it can be difficult to get names in some small ccTLDs to resolve at all.[92] In that context, the problems presented by wildcards do not loom large. The situation is different in COM, whose infrastructure is effectively that of the internet itself.

In response to Site Finder, different internet service providers adopted different workarounds. Most did nothing; they simply passed the Site Finder responses on to their users. Some applied the BIND patches released by ISC. Others adopted other creative responses to attack Site Finder's monopoly on interpreting "no such domain" messages.[93] Some networks programmed their routers to send users who would otherwise have hit the Site Finder web page to a different, revenue-generating web page set up by the internet service provider.[94] Indeed, a couple of very large access providers not only mapped the Site Finder web server's IP address to a local web page, but also imposed their own Site Finder-like functionality, sending users to a local search page, in connection with "no such domain" responses in *other* top-level domains.[95] This made the situation even more complicated and unhelpful.[96]

In the public debate, VeriSign representatives cast the question as whether VeriSign would be allowed to implement helpful, innovative changes in the internet infrastructure, making money that would enable more research and

---

89. Further, we need not worry much about the MUSEUM server being overwhelmed by the volume of HTTP requests or misaddressed email, and the tight restrictions on registration of those domains means that spam filters need not worry much about them. MUSEUM registrants have agreed to the wildcard, and are primarily focused on delivering web pages. See Museum Domain Management Association, *supra* note 88; see also Statement of John Klensin, SECSAC Meeting, *supra* note 67.

90. PH and CC have between 35,000 and 40,000 hosts apiece. See ISC, "Distribution of Top-Level Domain Names by Host Count" (January 2003), <http://www.isc.org/ds/WWW-200301/dist-bynum.html>.

91. While in theory, a ccTLD could use a wildcard to refer HTTP requests to a search page customized to local language and conditions, in my survey all eleven either resolved to some sort of advertising page or failed to resolve at all.

92. My email this morning, for example, contained a message noting that the MZ domain (Mozambique) is currently entirely inaccessible. T. Byfield, "[bwg+] .mz Falls Off the Map" (30 November 2003) (on file with author).

93. See Statement of Paul Vixie, SECSAC Meeting, *supra* note 67.

94. *Ibid.*; Paul Vixie, "Observed Workarounds to Synthetic Data Returned for Uninstantiated Names in .COM/.NET" *ICANN* (7 October 2003), <http://www.icann.org/presentations/vixie-secsac-dc-07oct03.ppt> [Vixie, "Observed Workaounds"].

95. See sources cited *supra* note 94. Vixie, in his testimony, stated that this was done by "a couple of…multi-million-user access providers." There are six ISPs in the United States with more than two million subscribers (America Online, MSN, United Online, EarthLink, Comcast, and SBC), and more outside the United States. See ISP-Planet Staff, "Top U.S. ISPs by Subscriber: Q2 2003" (8 September 2003), <http://www.isp-planet.com/research/rankings/usa.html>.

96. See "IAB Commentary," *supra* note 6 noting that Site Finder inspired other internet entities to undertake "hasty, possibly mutually incompatible and possibly deleterious (to the internet as a whole) changes to their own operations."

investment and thus a stronger internet, or whether technological purists would "hold the Internet back" by insisting that "the Internet world is flat and therefore there is no need for further exploration."[97] This misses the point. It is the stability of the core internet infrastructure—including the domain name system—that enables crucial internet innovation and investment in the services built on that infrastructure.[98] Site Finder undermined that stability.

*

3.

SHORTLY AFTER VERISIGN DEPLOYED Site Finder, people began urging that ICANN should force its withdrawal.[99] Within three weeks, that is exactly what happened: ICANN's formal demand and legal threats forced VeriSign to back down and withdraw the service. But did ICANN actually have that power? Had the matter gone to litigation against VeriSign, would it have prevailed? The matter is worth some analysis.

The first point that bears emphasis is that ICANN had no leverage at all unless VeriSign, in implementing Site Finder, was violating its registry contracts. In theory, that issue should not have been dispositive. The registry contracts were first executed in 1999 after arduous, three-way negotiations among ICANN, NSI (VeriSign's predecessor-in-interest), and the U.S. Department of Commerce, and then renegotiated in 2001. They recite that a two-thirds majority of the ICANN board of directors may adopt a "consensus policy"[100] binding registries, on an emergency basis, if it "reasonably determines that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the operational stability of Registry Services, the DNS or the Internet, and that the proposed specification or policy is as narrowly tailored as feasible to achieve those objectives."[101] Accordingly, even if VeriSign was not in violation, ICANN had authority to enact an emergency policy forbidding registry-level wildcards.[102] Given

---

97. Mark McLaughlin, Senior VP, VeriSign, "Innovation and the Internet" *CNET News.Com* (6 October 2003), <http://news.com.com/2010-1071-5086769.html>.

98. See Kevin Werbach, "What is Internet Infrastructure?" *WERBLOG* (17 October 2003), <http://werbach.com/blog/2003/10/17.html#a1267>.

99. See *e.g.* posting by Dave Farber, dave@farber.net, to ip@v2.listbox.com, "[IP] ICANN At-Large Advisory Committee Response to VeriSign 'SiteFinder' *Interesting-People* (16 September 2003), <http://lists.elistx.com/archives/interesting-people/200309/msg00151.html>.

100. ICANN's founders emphasized, at its creation, that it would act only through consensus. See Weinberg, *supra* note 5 at 250–51; letter from Esther Dyson to The Honourable Thomas J. Bliley, Jr., (8 July 1999), <http://www.icann.org/correspondence/dyson-letter-08july99.htm>. That language was incorporated into the registry and registrar contracts. See Weinberg, *supra* note 5 at 214 and n.140. Later on, ICANN's CEO came to the conclusion that "the original concept of a purely private sector body, based on consensus and consent, has been shown to be impractical." See Stuart Lynn, "President's Report: ICANN—The Case for Reform" *ICANN* (24 February 2002), <http://www.icann.org/general/lynn-reform-proposal-24feb02.htm>. That change of heart helped kick off a restructuring process and ICANN's adoption of new bylaws. See "Appendix A to Minutes of Board Meeting in Shanghai" *ICANN* (31 October 2002), <http://www.icann.org/minutes/minutes-appa-31oct02.htm>. However, the contractual provisions described in the text were not affected.

101. See ".com Registry Agreement," *supra* note 31 at § I.1.C.

102. Some observers called upon ICANN to do exactly that. See *e.g.* George Kirikos, "[ga] Re: Trailing Hyphen domains (and Security and Stability Statement, and the Language ICANN Needs In Its Contracts)" (22 September 2003), *ICANN/GNSO GNSO Email List Archives,* <http://gnso.icann.org/mailing-lists/archives/ga/msg00440.html>.

the IAB's reaction to Site Finder, and the SECSAC's initial reaction, establishment of an emergency policy on those grounds would have been more than plausible.

But that was only in theory. The contracts, carefully negotiated by NSI with an eye to limiting ICANN's ability to issue commands binding on it, also state that VeriSign has no obligation to comply with such an ICANN policy unless ICANN has established an Independent Review Panel pursuant to its bylaws, and VeriSign has either lost an appeal to that panel or declined to take one.[103] When ICANN rewrote its bylaws in 2002, it abolished its old (never implemented) Independent Review Panel, and provided instead that it would contract with an international arbitration provider to operate a new Independent Review Panel.[104] That provider had the job of establishing operating rules and procedures for the panel, subject to the ICANN board's approval.[105] ICANN, however, never entered into that relationship; it has no Independent Review Panel. As a practical matter, thus, it has no power to enact any new consensus policies binding any top-level domain registry.[106]

Some of those objecting to Site Finder urged that even if ICANN had no formal power to order VeriSign to discontinue Site Finder now, ICANN could surely decline to renew VeriSign's contracts to manage the COM and NET registries when those contracts came up for renewal.[107] Yet those contracts (again, not coincidentally; this language was carefully negotiated by VeriSign) are crystalline that ICANN *may not* decline to renew VeriSign's registry contracts unless: (1) VeriSign is in material breach of its contractual obligations; (2) ICANN reasonably determines that VeriSign, as registry operator, "has not provided and will not provide a substantial service to the Internet community;" (3) VeriSign is "not qualified" to serve as registry operator during the renewal term; or (4) VeriSign plans to charge consumers an unreasonable fee for registrations once its contract is renewed.[108] Thus, as a practical matter, nothing in the Site Finder affair empowers ICANN to decline to renew either the NET or the COM registry contracts unless some aspect of Site Finder implementation puts VeriSign in material breach of the registry contracts.

Was VeriSign in breach? Complainants were quick to answer yes.[109] Some pointed to the contract provisions[110] obligating VeriSign to follow three key internet standards documents describing the domain name system,[111] and

---

103. See ".com Registry Agreement," *supra* note 31 at § I.1.(A), (F).
104. See "ICANN Bylaws," *supra* note 52 at art. IV, § 3.
105. *Ibid.*
106. See Jonathan Weinberg, "Why VeriSign Isn't Worried" *ICANNWATCH* (24 September 2003), <http://www.icannwatch.org/article.pl?sid=03/09/24/226215>.
107. See *e.g.* Sean Donelan, "When is VeriSign's Registry Contract Up for Renewal" (22 September 2003), <http://www.irbs.net/internet/nanog/0309/1015.html>.
108. See ".com Registry Agreement," *supra* note 31 at § II.25.
109. See *e.g.* Steven Heath, "RE: [ga] More on Site Finder Suspension" (24 September 2003), *ICANN/GNSO GNSO Email List Archives*, <http://gnso.icann.org/mailing-lists/archives/ga/msg00464.html>.
110. "Revised VeriSign Registry Agreements: Appendix C" *ICANN* (16 April 2001), <http://www.icann.org/tlds/agreements/VeriSign/registry-agmt-appc-16apr01.htm#4> at element 4.
111. See Paul Mockapetris, Request for Comments: 1034, "Domain Names—Concepts and Facilities" *Internet Engineering Task Force* (November 1987), <http://www.rfc-editor.org/rfc/rfc1034.txt> ["RFC 1034"]; Mockapetris, "RFC 1035" *supra* note 6; Robert Elz *et al.*, Request for Comments: 2182, "Selection and Operation of Secondary DNS Servers" *Internet Engineering Task Force* (July 1997), <http://www.rfc-editor.org/rfc/rfc2182.txt>. All three documents, part of the humbly-titled RFC (Request for Comment) series, are internet standards adopted by the Internet Engineering Task Force. See Weinberg, *supra* note 5 at 193.

urged that Site Finder violated those standards documents. Specifically, some argued, RFC 1035 obligates a zone server to return a "no such domain" message whenever the domain name referenced in the query does not exist.[112] Site Finder does not do that. This argument seems untenable, though, in light of RFC 1034's explicit contemplation that a zone server *may* use wildcards to synthesize resource records, and thus return a response other than an error message for an otherwise-nonexistent domain.[113] The problem with Site Finder was not that VeriSign implemented wildcards to avoid returning NXDOMAIN messages; the problem was that it did so in a manner that interfered with the proper functioning of existing applications and was architecturally undesirable.[114]

A stronger argument relies on a functional characterization of what Site Finder did. As Jonathan Zittrain wrote, "isn't Site Finder a functional assignment by VeriSign of all previously-nonregistered domain names to itself?"[115] When VeriSign implemented Site Finder, it inserted a line in the registry database corresponding to the name "*.COM". Because of the asterisk, this line matched *any* domain name ending in .COM that did not otherwise exist in the registry,[116] and returned the IP address associated with the Site Finder server. Thus, at VeriSign's direction, all previously-nonregistered names resolved to VeriSign, displaying a VeriSign web page in response to an HTTP request.[117] A "dig" query (which requests basic DNS records) for any of those names returned an IP address corresponding to the Site Finder server, controlled by VeriSign. It is true that VeriSign would relinquish any of those names to a would-be registrant armed with payment. Nonetheless, the arguable effect of the wildcard was to make VeriSign walk, act and quack like the effective registrant of *every* character string in the COM and NET registries not registered by somebody else.

This reasoning is a little dicey, and arguments could surely be made the other way. The effect of the wildcard was to generate only a very limited set of resource records for each unregistered name. The wildcard synthesized only an A record, containing the IP address of the Site Finder server. It did not generate any nameserver (NS) records, identifying nameservers that were authoritative for the names. But it is hardly crazy to think that VeriSign was effectively registering the names. After all, not only did HTTP requests for the names resolve on its server, but it was making money from users' clicks on the directory links within those pages. Its relationship to the names seems not too different from that of

---

112. In its listing of response codes, the document specifies RCODE 3 as "Name Error—Meaningful only for responses from an authoritative name server, this code signifies that the domain name referenced in the query does not exist." Mockapetris, "RFC 1035," *supra* note 6, sec. 4.1.1 at 26.

113. See Mockapetris, "RFC 1034," *supra* note 111, s. 4.3.3 at 24–25. The discussion begins:

> RRs [resource records] with owner names starting with the label "*"…are called wildcards. Wildcard RRs can be thought of as instructions for synthesizing RRs. When the appropriate conditions are met, the name server creates RRs with an owner name equal to the query name and contents taken from the wildcard RRs. This facility is most often used to create a zone which will be used to forward mail from the Internet to some other mail system…

114. See "IAB Commentary," *supra* note 6 which emphasizes that Site Finder—though dangerous, highly problematic, and inconsistent with "the operational stability of the applications which depend on the DNS"—nonetheless "did not in any way violate the DNS specifications themselves."

115. Jonathan Zittrain, "VeriSign's Site Finder & ICANN Contracts—A Second Opinion" *ICANNWATCH* (25 September 2003), <http://www.icannwatch.org/article.pl?sid=03/09/25/223232>.

116. See Mockapetris, "RFC 1034," *supra* note 111 at s. 4.3.3.; "IAB Commentary," *supra* note 6.

117. "IAB Commentary," *supra* note 6.

the typosquatter that erects a pay-per-click search page at a domain name similar to an oft-requested one—say, googgle.com. By virtue of the wildcard, one could argue, VeriSign was typosquatting on *all* otherwise-unregistered names in COM and NET.

The VeriSign registry agreement for COM, moreover, is amenable to this reading. It defines "Registered Name" to include "a domain name within the domain of the Registry TLD…about which Registry Operator…maintains data in a Registry Database."[118] ("Registry Database," in turn, is defined to mean "a database comprised of data about one or more DNS domain names within the domain of the Registry TLD that is used to generate…DNS resource records that are published authoritatively or [whois data].")[119] The question in this context is whether VeriSign is deemed to "maintain data" in its database about the wildcarded names; the answer is, at least arguably, yes.[120]

If one accepts this argument, the consequences are far-reaching. The registry, under this argument, has effectively registered millions of names on its own behalf. That would stand in clear violation, though, of the registry-registrar relationship embodied in the contracts. The contracts reflect an institutional structure in which registrars register names and submit the appropriate data to the registry. Registries are neutral among the various registrars, not favouring one above the other. They do not themselves allocate names to the public and can register names on their own behalf only in exceptional cases.

Section 24 of the registry agreement for COM, thus, in conjunction with Appendix X, forbids VeriSign to register any domains "other than on a request submitted by a registrar pursuant to that registrar's Registry-Registrar Agreement."[121] Section 23 and Appendix I forbid VeriSign to "in any way attempt to warehouse, or register domain names in its own right other than through an ICANN-accredited registrar," forbid it to act as a registrar except pursuant to structural separation, and require it to provide all registrars with equivalent access, absent any preference or special consideration.[122] Section 20

---

118. ".com Registry Agreement," *supra* note 31 at § I.6. The definition continues: "A name in a Registry Database may be a Registered Name even though it does not appear in a TLD zone file (e.g., a registered but inactive name)."

119. *Ibid.* at § I.8.

120. VeriSign redirected to Site Finder not only unregistered names, but also domain names on registrar hold or in the redemption grace period, as well as any domain name without nameservers. See "Advisory Concerning Demand to Remove VeriSign's Wildcard" *ICANN* (3 October 2003), <http://www.icann.org/announcements/advisory-03oct03.htm> ["Advisory"]; Letter from Register.com to VeriSign (19 September 2003), <http://www.icann.org/correspondence/registercom-to-VeriSign-19sep03.pdf>; John Berryhill, "It Is Not Just Unregistered Names" *ICANNWATCH* (17 September 2003), <http://www.icannwatch.org/comments.pl?sid=1409&cid=12230>. All of those are surely "Registered Names;" the question then becomes whether we deem them to have been effectively re-assigned to VeriSign.

121. ".com Registry Agreement," *supra* note 31 at § II.24, Appendix X. Specifically, section 24 reads: "Registry Operator may register the domain names listed on Appendix X (Part A) for its own use in operating the registry and providing Registry Services under this Agreement, provided the total number of domain names listed on Appendix X at any time does not exceed 5000." Appendix X, in turn, reads: "The domains to be registered by Registry Operator, other than on a request submitted by a registrar pursuant to that registrar's Registry-Registrar Agreement, are as follows: None at this time." Some registry agreements do allow the registry to register a significant number of names on its own behalf; see ".info Registry Agreement" *ICANN* (25 May 2001) at Appendix X, <http://www.icann.org/tlds/agreements/info/registry-agmt-appx-11may01.htm> (listing 150 domain names to be registered by the INFO registry) [".info Registry Agreement"]. Even there, though, the registry can register no names on its own behalf other than those specifically listed in the agreement.

122. ".com Registry Agreement," *supra* note 31 at § II.23, Appendix I.

requires it to accept names for registration only pursuant to a registry-registrar protocol set out in Appendix C.[123]

If we deem VeriSign to have effectively registered all unassigned names, then it was in violation of all of these provisions. That is the view reflected in ICANN's October 3 demand, which complained of "violation of the Code of Conduct [Appendix I] and equal access obligations agreed to by VeriSign, failure to comply with the obligation to act as a neutral registry service provider, failure to comply with the Registry Registrar Protocol, [and] failure to comply with domain registration limitations."[124]

Three words in the ICANN demand, however, reflect a separate, and somewhat curious, argument: the letter and advisory complain that Site Finder is an "unauthorized Registry Service."[125] This is odd because the contract does not on its face require that ICANN approve registry services as such. By virtue of the contract's Appendix G, VeriSign must obtain ICANN approval before *charging* for a new registry service. Indeed, Appendix G states that VeriSign "shall not be entitled to charge for any Registry Service" other than registering, renewing and transferring names.[126] In conjunction with the dispute over the applicability of Appendix G to VeriSign's proposed Wait List Service,[127] ICANN staff took the view that a "registry service" is one "provided as an integral part of the operation of the Registry TLD": it is a service "that a registry operator is enabled to provide on a sole-source basis by virtue of" its status as registry operator, rather than one provided on a competitive basis.[128] By this reasoning, Site Finder surely seems like a registry service. But the fact remains that VeriSign did not charge users to access the Site Finder site. Appendix G, thus, does not apply, unless one deems VeriSign to have provided a new, paid, registry service to Overture, Inc., the company that administered the directory links on the Site Finder web site and returned money to VeriSign when users clicked through to Overture clients via the Site Finder links.[129]

In sum, ICANN had leverage over Site Finder only if VeriSign was violating the terms of its registry contracts. It was in a position to make two sets of arguments that VeriSign was doing just that. The first—that Site Finder allowed VeriSign to enjoy the effective registration of all unassigned names on its own behalf—was plausible and even appealing, but hardly a slam-dunk. The second—that VeriSign was charging for an unapproved "registry service" when it contracted with Overture to place links on the Site Finder web site and agreed to be paid on a click-through basis—was possible, but again less than self-evident.

---

123. *Ibid.* at § II.20. "Unless and until ICANN adopts different standards as a Consensus Policy pursuant to Definition 1 and Section 3, Registry Operator shall provide Registry Services to ICANN-accredited registrars in a manner that meets the performance and functional specifications set forth in Appendices C and D…"

124. "Advisory," *supra* note 120.

125. *Ibid.*

126. ".com Registry Agreement," *supra* note 31, Appendix G.

127. See *infra* note 135 and accompanying text.

128. "ICANN Bucharest Meeting Topic: VGRS Proposal for Wait-Listing Service" *ICANN* (19 May 2002), <http://www.icann.org/bucharest/wls-topic.htm>. Accordingly, it continued, VeriSign could not charge for the Wait List Service, absent amendment of the registry agreement.

129. See *supra* note 11 and accompanying text.

Their combined force helped convince VeriSign to back down. But neither derived much force from the key architectural concerns that I stressed in the previous section. The registry contracts gave ICANN no hook to invoke those concerns. If VeriSign was in breach, it was by happenstance.

4.

ICANN TAXONOMY DIVIDES the generic top-level domain registries into "sponsored" and "unsponsored" groups. The sponsored registries—AERO, COOP, EDU, and MUSEUM—are non-profit and, in theory, have institutional structures that make them responsive to their registrants.[130] All but one of the unsponsored registries—COM, NET, ORG, INFO, BIZ, NAME, and PRO—are profit-driven and open to registration by the community at large.[131] The sponsored registries are not subject to ICANN price regulation; rather, their contracts specify that "any revenues received by Sponsor…from the provision of Registry Services are used solely for the benefit of the Sponsored TLD Community."[132] By contrast, the registry contracts for the unsponsored registries directly regulate prices for registry services,[133] and Appendix G of those contracts prohibits the registry operator from charging for a new registry service without ICANN's approval."[134]

In 2001, well before Site Finder, VeriSign submitted a controversial proposal to ICANN. VeriSign proposed to implement a "Wait List Service" under which the registry would allow customers to reserve the rights to register domain names currently held by others, should the current holders let the names

130. ICANN also lists GOV and MIL as "sponsored" by the U.S. Government. See <http://www.icann.org/tlds/>.

131. ORG is now operated by the Public Interest Registry, a nonprofit corporation. See "PIR Articles of Incorporation," <http://www.isoc.org/dotorg/pir-articles.shtml>. ICANN also lists INT as an unsponsored domain (see <http://www.icann.org/tlds/>), but it is rather a special case; while it has no sponsoring organization, it is used only for registering organizations established by international treaties between or among national governments. See <http://www.iana.org/int-dom/int.htm>.

132. See *e.g.*, "TLD Sponsorship Agreement: Attachment 2 (.museum)" *ICANN* (20 August 2001), <http://www.icann.org/tlds/agreements/museum/sponsorship-agmt-att2-20aug01.htm>.

133. ICANN exerts its control over registry pricing, and a wide range of other aspects of registry business, through the mechanism of the detailed contracts it has signed with each registry as a condition of access to the root. It is hard to characterize this as anything other than "regulation." See Jonathan Weinberg, "ICANN, Internet Stability, and New Top Level Domains" in, Lorrie Cranor & Shane Greenstein, eds., *Communications Policy and Information Technology: Promises, Problems, Prospects* (Cambridge: MIT Press, 2002) 4. But see Thomas Roessler, "New Registry Services, and Other Changes" (23 October 2003), <http://log.does-not-exist.org/archives/000853.html> (reporting comments of Jeff Neumann).

134. See ".biz Registry Agreement: Appendix G" *ICANN* (18 June 2003), <http://www.icann.org/tlds/agreements/biz/registry-agmt-appg-18jun03.htm>; ".com Registry Agreement: Appendix G" *ICANN* (16 April 2001), <http://www.icann.org/tlds/agreements/VeriSign/registry-agmt-appg-com-16apr01.htm>; ".info Registry Agreement: Appendix G" *ICANN* (11 May 2001), <http://www.icann.org/tlds/agreements/info/registry-agmt-appg-11may01.htm>; ".name Registry Agreement: Appendix G" *ICANN* (8 August 2003), <http://www.icann.org/tlds/agreements/name/registry-agmt-appg-8aug03.htm>; ".net Registry Agreement: Appendix G" *ICANN* (16 April 2001), <http://www.icann.org/tlds/agreements/VeriSign/registry-agmt-appg-net-org-16apr01.htm>; ".org Registry Agreement: Appendix G" *ICANN* (19 August 2003), <http://www.icann.org/tlds/agreements/org/registry-agmt-appg-19aug03.htm>; ".pro Registry Agreement: Appendix G" *ICANN* (27 April 2002), <http://www.icann.org/tlds/agreements/pro/registry-agmt-appg-27apr02.htm>. In most of these agreements, the contracts flatly prohibit the introduction of any registry service not specified in Appendix G, so that ICANN approval must come in the form of a modification of the agreement.

expire.[135] By virtue of Appendix G, VeriSign needed ICANN's go-ahead in order to begin. ICANN puzzled over how to exercise its contractual power. It had "not yet developed a well-defined procedure for considering requests by registry operators to amend Appendix G to allow charging for an additional registry service."[136] Its general counsel, Louis Touton, suggested at the time that any procedural mechanism would have to balance the potential harm to others posed by the service against the stifling effect on innovation of requiring a consensus-development process for every new registry service.[137] To accommodate those concerns, Touton suggested that ICANN approve the service using a streamlined process so long as a preliminary "quick-look" evaluation suggested that it would not harm others' legitimate interests, but that it invoke formal consensus mechanisms if there were "specific reasons to conclude that the legitimate interests of others are likely to be harmed."[138] In the end, ICANN approved the Wait List Service notwithstanding strenuous outcry against it.[139]

In the wake of the Site Finder affair, ICANN CEO Paul Twomey drew a connection between Site Finder and ICANN's review of the Wait List Service. The contract provisions barring the offering for a fee of any registry service not specified in the agreement, he stated, had come into play in connection with both services.[140] "Our experience to date," he continued, "makes it clear that there is a need for more thought to be given to the appropriate processes to be followed in such cases in the future, and in analogous circumstances that might have similar effects."[141]

Accordingly, in the same documents in which ICANN enunciated its formal demand to VeriSign to shut down Site Finder, Twomey took the first step to put in place, through ICANN's policy development process, a new "timely, transparent and predictable procedure for the introduction of new registry services."[142] As this article went to press, ICANN staff published an "issue report" setting out staff's understanding of how the new process should work.[143] ICANN's agreements with the top-level domain registries, the report stated, include a variety of constraints on the ability of the registry operator or sponsor[144] to make changes

---

135. The proposal was controversial in part because of the threat it posed to a set of enterprises currently engaged in snapping up domain names as they expired and reselling them to interested customers. In the words of one reporter, "[t]hat crashing sound you hear is the sound of an entire niche industry collapsing." Jim Wagner, "ICANN Approves Waiting List Service" *internetnews.com* (25 August 2002), <http://www.internetnews.com/xSP/article.php/1451891>.

136. "General Counsel's Analysis of VeriSign Global Registry Services' Request for Amendment to Registry Agreement" *ICANN* (17 April 2002), <http://www.icann.org/minutes/report-vgrs-wls-17apr02.htm>.

137. *Ibid.*

138. *Ibid.*

139. A court recently rejected a lawsuit against ICANN seeking to set aside that approval. ICANN was not obligated to generate a new "consensus policy" before approving the service, the court reasoned, because doing so would not create new obligations running from unwilling registries or registrars to ICANN. See Order Denying Plaintiff's Motion for Preliminary Injunction, *Dotster, Inc. v. ICANN*, No. CV 03-5045-JFW (MANx) (C.D. Cal. 2003), available at <http://www.lextext.com/dotsterPIOrder.tif>.

140. *Supra* note 55.

141. *Ibid.*

142. *Supra* note 120.

143. Staff Manager's Issue Report, *supra* note 3. The issue report is step two of ICANN's fourteen-step Policy Development Process for generic domain names. See ICANN Bylaws, Annex A, <http://www.icann.org/general/bylaws.htm#AnnexA>.

144. The entity setting policy for a sponsored domain is a "sponsor"; the actual work of maintaining the registry will likely be undertaken by a different firm, referred to as the "operator." An unsponsored top-level domain has only an operator. See <http://www.icann.org/tlds/>.

in the registry's architecture or operation without ICANN's consent.[145] In the past, the report continued, those matters had been handled via the sort of process described above in connection with the Wait List Service.[146] Yet "[t]he current procedure could be substantially improved—in terms of both clarity and predictability."[147] Thus, the report concluded, it is desirable to establish a standardized process to govern such ICANN approvals. Although the document is a little unclear on the point, it appears to state that the new process should cover not merely actions for which the existing contracts require ICANN approval, but indeed *all* "significant actions by TLD registries that, because of their architecture or operation, could affect the operational stability, reliability, security or global interoperability of the DNS, that registry, or the Internet."[148] The issue report does not explain the basis for that expanded scope, except by describing it as "reality" that "any proposed changes that could have the effects described should be subject to an appropriate consideration process."[149]

To the extent that the new policy development process is simply aimed at clarifying how ICANN should exercise its existing contractual power over new paid services offered by the unsponsored registries, ICANN's authority is not problematic. But the report seems to contemplate that the process will also cover services offered by sponsored registries,[150] and changes that are not "services" at all. If ICANN asserts such power, it will go beyond its existing contracts. The sponsored registry contracts contain no such approval requirement, and explicitly disclaim any ICANN authority over "[f]unctional and performance specifications for, and pricing of, Registry Services."[151] Even when it comes to unsponsored registries, the contracts give ICANN no review authority in connection with most actions by the registries other than the introduction of paid registry services.

Presumably, ICANN could extend its authority over sponsored and unsponsored registries alike by enacting an appropriate consensus policy.[152] But there are a variety of obstacles along that path. The first derives from ICANN's rhetorical sleight of hand; rather than seeking to generate a consensus for extending its authority over registry actions, it appears to be trying to give the inaccurate impression—without ever engaging in bald misstatement—that it has

---

145. Staff Manager's Issue Report, *supra* note 3.

146. See *supra* note 135 and accompanying text.

147. Staff Manager's Issue Report, *supra* note 3.

148. *Ibid.*

149. *Ibid.*

150. At one point, thus, the report refers to the contemplated process as one "by which ICANN considers *operator or sponsor* requests." *Ibid.* [emphasis added]. On the distinction between the two, see *supra* note 144.

151. See "TLD Sponsorship Agreement: Attachment 2 (.museum)" *ICANN* (20 August 2001), <http://www.icann.org/tlds/agreements/museum/sponsorship-agmt-att2-20aug01.htm>; Thomas Roessler, "What's Really in That Issues Report?" (20 November 2003), <http://log.does-not-exist.org/archives/000990.html>.

152. ICANN can enact domain-name consensus policies, see *supra* notes 100–106 and accompanying text, on a non-emergency basis via written documentation evidencing that the policy enjoys sufficient "consensus among Internet stakeholders represented in the ICANN process," a two-thirds vote of the Generic Names Supporting Organization Council, and an affirmative vote of the ICANN Board. See ".com Registry Agreement," *supra* note 31 at §I.1. The unsponsored registries have suggested, obliquely, that this particular consensus policy might be inconsistent with their contracts. See Ken Stubbs, "[council] FWD: UNSPONSORED REGISTRIES STATEMENT—Regarding the Proposed Issues Report on Registry Services" (7 November 2003), *ICANN/GNSO GNSO Email List Archives*, <http://www.gnso.icann.org/mailing-lists/archives/council/msg00283.html>.

the authority already. Another relates to a point I mentioned earlier in a different context: Because ICANN hasn't established an independent review process, it can't in any event impose a consensus policy on an unwilling registry.[153] Finally, and most importantly, it's by no means clear that ICANN can get support for such a policy. As this article goes to press, Bruce Tonkin, chair of the Generic Names Supporting Organization Council,[154] has prepared a draft Terms of Reference for the policy development process that emphatically foreswears any extension of ICANN authority over registries beyond those cases in which contractual authority already exists.[155] And there is reason to believe that the Generic Names Supporting Organization Council, as a whole, agrees.[156] No generic-domain-name consensus policy can be enacted without the two-thirds support of the GNSO Council.[157]

How far should ICANN's regulatory power (whether based in contract or otherwise) extend in this arena? Should there be a process in which staff evaluate the introduction of new registry services or other registry actions, and turn thumbs down on those found wanting? I approach the proposal with a good deal of scepticism. I will argue in the rest of this paper that *l'affaire Site Finder* should not be the occasion to extend ICANN regulatory power throughout the universe of top-level domain registries.

Let's start with the policy issues implicated by existing ICANN review of new registry services. As I've noted, the registry contracts for all of the unsponsored generic top level domains regulate prices for registry services and prohibit the registry operator from charging for a new registry service without ICANN's approval.[158] Is this appropriate? A partial rationale for the restriction springs fairly readily to mind. All but one of the unsponsored registries are for-profit and thus have an incentive to charge profit-maximizing prices. A registry exercises significant market power over its registrants by virtue of "lock-in:" a registrant with a well-established domain name would incur substantial costs in moving to a different registry and, thus, a different domain name.[159] To the extent of those costs, a registry can charge registrants inefficiently high renewal prices unless restrained by ICANN price regulation, and price regulation implies some sort of oversight mechanism.

On the other hand, this rationale is not really sufficient to explain all of ICANN's regulation of registry services. ICANN regulates prices for the initial

---

153. See *supra* notes 103–106 and accompanying text.

154. Tonkin is Chief Technology Officer of registrar Melbourne IT and also chair of VeriSign's internal Site Finder technical advisory panel. See Bruce Tonkin, "[council] Update on Declaration of Conflict of Interest" (2 October 2003), *ICANN/GNSO GNSO Email List Archives*, <http://www.gnso.icann.org/mailing-lists/archives/council/msg00156.html>.

155. Bruce Tonkin, "[council] Draft Terms of Reference on ICANN Procedure for Approving Contractual Approvals or Amendments Related to the Operations of a gtld Registry" (21 November 2003), *ICANN/GNSO GNSO Email List Archives*, <http://www.gnso.icann.org/mailing-lists/archives/council/msg00307.html>.

156. See Thomas Roessler, "Yesterday's Council Call" (21 November 2003), <http://log.does-not-exist.org/archives/000994.html>.

157. See *supra* note 152.

158. See *supra* note 134.

159. See U.S., Department of Commerce, *Comment of the Staffs of the Bureaus of Economics and Competition of the Federal Trade Commission before the National Telecommunications and Information Administration* (S. Doc. No. 980212036-8036-01) (Washington, D.C.: 1998), <http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/scanned/FTC.htm>.

registration of a name.[160] Lock-in does not apply there. The same is true for the initial registrations of "multilingual" names (that is, domain names incorporating non-ascii characters), where ICANN has authorized them.[161] The rationale for this category of regulation here must be a different one: that unsponsored registries have market power simply by virtue of the scarcity of attractive, open registries in the domain name space.

There is a profound irony here: Because of the market dominance of COM and NET, and because there are so few unsponsored registries at all, we see a need for ICANN regulation to address the registry's market power. But it is ICANN that has maintained that top-level domain scarcity. As long ago as 1996, Jon Postel (the USC computer scientist who served as overseer of the domain name space) proposed adding as many as 150 new generic top-level domains.[162] The story of why we still have so few is a long and sorry one, too long to tell here.[163] The bottom line, though, is that "regulatory choices by ICANN…have persistently limited the number of gTLDs to levels far below those warranted by any technical requirements."[164] That limit on the number of generic top-level domains has helped cement VeriSign's market power. ICANN's regulatory imperative, in short, flows from its own policy choices.[165]

ICANN, moreover, regulates prices that registries charge *non*-registrants for services, in contexts where the registry does not seem to exert worrisome market power. The INFO registry contract recites the registry's plans to make available, "based on customer demand and technical feasibility," enhanced Whois searches (using Boolean and character string technology) and the ability to search the Whois database using LDAP (Lightweight Directory Access Protocol) clients.[166] It then indicates that the prices for all of these services are to be negotiated with ICANN.[167] But there is no reason to think that market pricing for these services would not be satisfactory.

All this is all the more troubling because of the problematic nature of ICANN regulation. As a general rule, ICANN should not regulate without good cause. We should be wary of imposing regulation unless we are sufficiently confident that it is necessary. Yet ICANN has shown a distressing tendency to micromanage and over-regulate. The contracts it negotiated two years ago with the

---

160. See *e.g.*, ".com Registry Agreement, Appendix G," *supra* note 134, ("Registry Operator may charge a maximum of US$6.00 per year for registration of each Registered Name (the 'Initial Registration Fee') in the Registry TLD.")

161. See ".biz Registry Agreement, Appendix G," *supra* note 134 (not only forbidding the registry to charge more for multilingual domain name renewals than it does for initial registration, but also compelling the registry to negotiate with ICANN its price for initial registration). For a different example, see the ".info Registry Agreement, Appendix G," *supra* note 134. The .info agreement sets the price the registry may charge for monitoring the registration of domain names similar to a registrant's trademark.

162. Jon Postel, "Internet Draft: New Registries and the Delegation of International Top-level Domains" *Internet Engineering Task Force* (August 1996), <http://www.mit.edu/afs/athena/reference/rfc/draft-postel-iana-itld-admin-02.txt> at ss. 5.6, 6.1; Weinberg, *supra* note 133.

163. For background, see sources cited *supra* note 5 along with Weinberg, *supra* note 133.

164. Karl Mannheim & Lawrence Solum, "The Case for gTLD Auctions: A Framework for Evaluating Domain Name Policy" (2003) Loyola-LA Public Law Research Paper No. 2003-1, <http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID388780_code030324530.pdf?abstractid=388780>, at 45.

165. Weinberg, *supra* note 133.

166. ".info Registry Agreement, Appendix G," *supra* note 134.

167. *Ibid.*

new registries were extraordinarily detailed, each about two inches thick in hard copy, specifying many aspects of the new registries' operations.[168] A requirement that ICANN approve all new registry service offerings, on a case-by-case basis, is likely to promote bureaucracy and stall innovation. A *prior* approval requirement, in particular, would make it easier, and hence more likely, for ICANN to rule against the introduction of a new service, and it would tend to instill in ICANN staff what Thomas Emerson described as the attitude of the censor, who "has a professional interest in finding things to suppress."[169]

Moreover, while ICANN's legitimacy is more firmly established than it was a few years ago, it is hardly beyond dispute.[170] It remains to be seen whether ICANN's most recent staffing change[171] and the most recent iteration of its bylaws[172] will put people at the helm whom the internet community will accept as appropriate wielders of authority in connection with the DNS. Finally, because ICANN is an industry cartel, any ICANN action subjecting new registry services to the proposed approval requirement has implications for competition policy and antitrust law. ICANN's Board, perhaps too cozily, includes representatives of both the registries and registrars. The new service approval process would often amount to deciding the extent to which one set could keep the other out of particular markets.[173]

Notwithstanding all of the above, I think that ICANN's role vis-a-vis Site Finder was a Good Thing. Site Finder interfered with basic internet architecture in a way that no other institution could adequately address. To be sure, the internet technical community reacted almost immediately, generating with blinding speed a series of patches and work-arounds to undo Site Finder's effects. This was in the best internet tradition. To paraphrase John Gilmore, the Net was interpreting Site Finder as damage and routing around it.[174] It appears, though, that the beneficial effects of the routing were limited.

For one thing, although ISC was responding to "high demand from [its] users,"[175] there is evidence that not many large networks applied the BIND patch. One careful study, looking for evidence that large networks had applied the patch, found it in connection with networks serving a total of no more than 10% of the world's internet users.[176] More than half of those users were in the

---

168. See Weinberg, *supra* note 133 at 4.

169. Thomas I. Emerson, "The Doctrine of Prior Restraint" (1955) 20 Law & Contemp. Probs. 648 at 659.

170. See Froomkin, "Wrong Turn," *supra* note 5; Weinberg, *supra* note 5.

171. I refer to the appointment of Paul Twomey as President/CEO in March 2003. See <http://www.icann.org/biog/twomey.htm>.

172. See "ICANN Bylaws," <http://www.icann.org/general/archive-bylaws/bylaws-26jun03.htm>.

173. See Jeff Neuman, "[council] FW: Statement of New Registry Services PDP" (13 October 2003), *ICANN/GNSO GNSO Email List Archives,* <http://www.gnso.icann.org/mailing-lists/archives/council/msg00173.html>. On the other hand, this sort of conflict is endemic to ICANN processes, and does not without more render its activities illegal. See A. Michael Froomkin & Mark A. Lemley, "ICANN and Antitrust" (2003) U. Ill. L. Rev. 1. Moreover, the Board would not be directly involved in the process, which presumably would be undertaken by ICANN staff.

174. The actual quotation, attributed to Gilmore although generally unsourced, is: "The Net interprets censorship as damage and routes around it." See the Internet Quotation Appendix (1990), <http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html>; Reagle, *supra* note 25.

175. "ISC Bind," *supra* note 18.

176. Jonathan Zittrain & Ben Edelman, " Technical Responses to Unilateral Internet Authority: The Deployment of VeriSign 'Site Finder' and ISP Response" (6 October 2003), available at <http://cyber.law.harvard.edu/tlds/sitefinder>.

People's Republic of China.[177] The researchers were able to find almost no large networks in the United States that had applied the patch.[178] They do note that Adelphia, which disabled Site Finder on September 19, re-enabled it four days later. They speculate that pressure from VeriSign may have motivated that move.[179] In general, the data is consistent with the hypothesis that while internet service provider technical staff were enthusiastic about disabling Site Finder, upper management at large commercial ISPs were more comfortable with the conservative approach of accepting whatever responses VeriSign served up.

For another, there is evidence (somewhat in conflict with the study above)[180] that a variety of internet service providers implemented responses to Site Finder that were no better from an architectural perspective, or even worse. As already noted, some networks responded by programming their routers to send users typing nonexistent domain names in COM and NET to a revenue-generating web page set up by the ISP. There is reason to believe that two very large access providers took the occasion to do the same thing in connection with "no such domain" responses in *all* top-level domains.[181] The IAB summed up the overall set of ISP responses to Site Finder as "hasty, possibly mutually incompatible and possibly deleterious (to the internet as a whole)…".[182] That does not look like usefully routing around damage.

It may be that the technical community's response would have been more effective had Site Finder been in operation for a couple of months or so.[183] As nameserver operators upgraded to BIND 9 over time (or installed versions of BIND 8 that they had received in a Linux or BSD distribution with the patch already applied),[184] they would have the ability to block Site Finder simply by configuring their software to do so. It may be that large ISPs did not block Site Finder before October 3 because they were waiting for ICANN to act, and that absent ICANN action they ultimately would have applied the ISC patch. But I don't find the evidence summarized above encouraging in that regard; indeed, it appears that some large networks were able to react very quickly indeed, but not in the direction of allowing end-user computers to get NXDOMAIN responses. And my own suspicion is that over time, the reaction to VeriSign's move would have become more muted rather than more aggressive, as Site Finder became more nearly a part of the landscape. So while we don't know for

---

177. *Ibid.*

178. *Ibid.* The authors did receive reports, which they were unable to confirm due to the nature of their data, that AOL disabled Site Finder as of September 19. See <http://cyber.law.harvard.edu/tlds/sitefinder/data1.html>.

179. *Ibid.*

180. On the one hand, there is testimony from Paul Vixie that two multi-million-user ISPs blocked users' access to Site Finder by sending them instead to a local web page set up by the ISP. See *supra* note 94 and accompanying text. On the other hand, such redirection ought to have been reflected in the Alexa data that formed the basis for the Zittrain & Edelman study described in text accompanying *supra* notes 176–179. Yet that study does not seem to list any networks that obviously look like the ones Vixie described.

181. See statement of Paul Vixie, SECSAC Meeting, *supra* note 67; Vixie, "Observed Workarounds," *supra* note 94 and accompanying text.

182. See "IAB Commentary," *supra* note 6.

183. I owe this reminder to Michael Froomkin.

184. See Statement of Paul Vixie, SECSAC Meeting, *supra* note 67 (noting that integrators such as Linux and BSD distributors had downloaded the patch).

sure, I'm doubtful that even with more time we would have returned anywhere near the pre-Site Finder status quo.

Nor can we feel confident about legal institutions' responses. While three lawsuits were filed against VeriSign (one of them, indeed, by a significant player in the domain name space),[185] suffice it to say that those suits are still wending their way through the court system at that system's usual glacial pace, and the prospect of such suits was apparently not a sufficient disincentive to stop VeriSign from implementing Site Finder in the first place. It is possible that VeriSign may yet get legal comeuppance at some point, but that result is by no means assured and is in any event distant. Legal institutions did not seem to provide any path toward a shorter-term regulatory response.

What do we learn from Site Finder about the direction ICANN should take for the future? First, that there is an additional irony in ICANN's regulation of registries so far. The contracts spill a great deal of ink micro-managing the registries' business models, but seem underdeveloped in the key area where an active ICANN role seems to make more sense. I suspect that we cannot avoid the sort of problem Site Finder posed simply by writing better prohibitions into the bodies of the contracts; I'm not sure what sort of contractual prohibition would have avoided Site Finder itself. At the same time, ICANN should not be imposing the same mechanisms on everyone. Most obviously, there is not a lot of advantage—and there is definitely the possibility of some harm—in establishing a requirement that ICANN must issue its blessing, on a case-by-case basis, before a small, non-profit, top-level domain registry can take standards-compliant action in its own corner of the Net.

The lesson of Site Finder is that there needs to be an effective institutional mechanism for protecting the infrastructure of the DNS—including both protocols embodied in the RFCs and key architectural assumptions—from unilateral change bypassing the protections and consensus mechanisms of the traditional internet standards process. Site Finder posed such a threat notwithstanding that it involved only a new implementation of existing standards in particular zone files. It posed that threat, most obviously, because of the sheer size and importance of VeriSign's zones, which included 60% of all internet hosts.[186] The change in the behaviour of the COM and NET zones amounted to a change in the basic infrastructure of the internet. Complicating this was the fact that VeriSign did not consider itself constrained by the traditional consensus practices that have animated internet standards development. Consensus practices, from VeriSign's standpoint, were the tools of people who do not "understand how to build products and promote markets."[187] The lesson of Site Finder, in short, is that the existing domain-name architecture and standards process are

185. GoDaddy.com is apparently the third largest registrar, in terms of market share in the five largest generic top-level domains plus .US. See RegistrarStats, "Daily Market Share Report" (12 November 2003), <http://www.registrarstats.com/>. This is not the first time Go Daddy has sued VeriSign; the earlier, unrelated, suit settled. Michael Singer, "VeriSign to Cease Mailings to All Registrars" *Internetnews* (20 June 2002), <http://www.internetnews.com/IAR/article.php/1369011>; "Go Daddy, VeriSign Settle Suit" *The Business Journal of Phoenix* (8 October 2002), <http://www.bizjournals.com/phoenix/stories/2002/10/07/daily23.html>.

186. See "Distribution by Top-Level Domain," *supra* note 9.

187. *Supra* note 2.

subject to substantial pressure from an aggressively for-profit VeriSign. Notwithstanding its failings, even a flawed ICANN may be better suited than any other existing institution to protect against that danger.

At the same time, whatever mechanism emerges from ICANN's policy development process should not apply beyond the realm where the danger is greatest: the six unsponsored registries. Indeed, there is merit to the suggestion that even within this group, the rules should be different for "dominant" and "non-dominant" players[188] (to borrow a term from communications law). It is unclear exactly how one might draw that line other than having VeriSign stand alone in the "dominant" category—but that result would not be so odd. VeriSign's registries do control a majority of all internet hosts, making a change in VeriSign's rules effectively a change in the infrastructure of the internet. Further, the rule would have some historical resonance.

The long process leading to ICANN's creation was sparked, after all, by concerns about the monopoly franchise that NSI, VeriSign's predecessor-in-interest, held to run the non-ccTLD portion of the domain name space.[189] To address that monopoly, ICANN at its creation was given two key jobs. One was to authorize a set of new generic top-level domains; it finally added a few of those in 2000. The other, though, was to introduce a system of competitive registrars to COM and the other top-level domains then administered by NSI. At the time, there was no registry-registrar split. NSI was the exclusive registrar for COM, NET, ORG and EDU.[190] ICANN was to administer a new regime in which NSI would develop a shared registration system allowing multiple registrars to register names within those top-level domains.[191] It was to accredit the new registrars[192] and ride herd, with backup from the Department of Commerce, on NSI's (notably recalcitrant) implementation of the transition to registrar competition.[193] In a very real sense, the United States government created ICANN to take over the responsibility to oversee NSI (now VeriSign) that the National Science Foundation was then abjuring. Given that VeriSign, as COM and NET registry, has maintained key authority over the largest portions of the DNS, it should not be so surprising that the need for a body to exercise that responsibility has not gone away.

---

188. See Milton Mueller, "[Council] Proposed Amendment to Resolution" (16 October 2003), *ICANN/GNSO GNSO Email List Archives*, <http://www.gnso.icann.org/mailing-lists/archives/council/msg00207.html>; "Draft Staff Manager's Issue Report for the Development of a Process for the Introduction of New or Modified Registry Services" *ICANN* (31 October 2003), <http://www.icann.org/gnso/issue-reports/draft-registry-svcs-report-31oct03.htm>, at s. 4.4.

189. See Testimony of Jonathan Weinberg, *Domain Name System Privatization: Is ICANN Out of Control? Hearings Before the Subcommittee on Oversight and Investigations of the House Committee on Commerce*, 106th Cong. (22 July 1999), available at <http://www.law.wayne.edu/weinberg/testimony.pdf> [Testimony of Jonathan Weinberg]; Weinberg, *supra* note 5 at 200–01.

190. See U.S., National Telecommunications and Information Administration, *Improvement of Technical Management of Internet Names and Addresses: Proposed Rule (the "Green Paper")*, 63 Fed. Reg. 8825, 8828 (1998), <http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm>.

191. See Amendment 11 to the DOC/NSI Cooperative Agreement, NCR-9218742 (7 October 1998), <http://www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm>.

192. See Mueller, *supra* note 5 at 186–88.

193. See Testimony of Jonathan Weinberg, *supra* note 189; Testimony of Esther Dyson, *Domain Name System Privatization: Is ICANN Out of Control? Hearings Before the Subcommittee on Oversight and Investigations of the House Committee on Commerce*, 106th Cong. (22 July 1999), available at <http://www.icann.org/correspondence/dyson-testimony-22jul99.htm>.

*

CONCLUSION

SITE FINDER TOOK THE FUNCTION of interpreting "no such domain" messages from client software, and built it into the infrastructure of the domain name system itself. It thus substituted monopoly for competition; it prevented the user from invoking any other service to deal with mistyped names no matter how far superior or better suited to particular user needs. It contravened key elements of internet architecture and undermined the stability of the core internet infrastructure. ICANN had leverage over Site Finder, though, only if VeriSign was violating the terms of its registry contracts. ICANN's arguments that Site Finder violated VeriSign's contractual obligations are plausible, but they do not derive their force from Site Finder's architectural or stability consequences. The registry contracts gave ICANN no hook to invoke those concerns; if VeriSign was in breach, it was by happenstance.

The lesson of Site Finder is that there needs to be an effective institutional mechanism for protecting the domain name space infrastructure from unilateral change that bypasses the protections and consensus mechanisms of the traditional internet standards process. The existing domain-name architecture and standards process are subject to substantial pressure from an aggressively for-profit VeriSign. Even a flawed ICANN may be better suited than any other existing institution to protect against that danger. Yet we should endorse ICANN regulatory authority only with extreme caution, and the same mechanisms should not apply to everyone. ICANN oversight should certainly not apply beyond the for-profit unsponsored registries. Even within this group, it may be that the rules should be different for "dominant" and "non-dominant" players—perhaps, for VeriSign and all others.