Masthead Logo

Global Business & Development Law Journal

Volume 21
Issue 1 *Symposium: I Think I Can, I Think ICANN: Regulating the Internet . . . or Not*

Article 6

1-1-2008

ICANN Can: Contracts and Porn Sites - Choosing "to Play Internet Ball in American Cyberspace"

Brent A. Little
Tenth Circuit Court of Appeals, 2007-08

Cheryl B. Preston
Brigham Young University

ICANN Can: Contracts and Porn Sites—Choosing "to Play Internet Ball in American Cyberspace"*

*Brent A. Little*** and Cheryl B. Preston****

TABLE OF CONTENTS

The World Wide Web has spread knowledge and economic opportunity around the globe, but as Richard A. Spinello observes, its remarkable growth "is not without its social costs."[1] The kind of pornography that was once available only to the most committed searcher is now just a click away from any Internet user, many of whom are minors. In many developing countries, the drive to train a new generation in technology skills as a foray into global commerce has produced an epidemic of pornography addiction that parents have no idea how to address.

Protecting children from Internet pornography is a global problem without a global answer. The borderless nature of the Internet makes coordinating responses extremely difficult. Individual countries are scrambling to find solutions. To combat pornography and other illegal online action, some countries

---

* Am. Online, Inc. v. Aol.org, 259 F. Supp. 2d 449, 457 (E.D. Va. 2003).

** Brent A. Little, Law Clerk to the Honorable Paul J. Kelly, Jr., Tenth Circuit Court of Appeals, 2007–08.

*** Cheryl B. Preston, Edwin M. Thomas Professor of Law, Brigham Young University. Thank you to Brian Christensen, Professor Margaret Tarkington, Christopher Reed, Daniel Adlong and Marin Bradshaw for research and comments.

1. RICHARD A. SPINELLO, CYBERETHICS: MORALITY AND LAW IN CYBERSPACE, at ix (3d ed. 2006).

are regulating Internet intermediaries such as Internet service providers (ISPs), information intermediaries such as Google or Blogger, or financial intermediaries such as credit card companies.[2] However, these efforts are not solving the problem. They are less effective in smaller countries where Internet intermediaries such as ISPs and financial institutions often do not have a presence or assets in that country.[3] Even larger and more powerful countries have difficulty controlling illegal online conduct where offenders minimize their dependence on intermediaries, thereby eliminating a government's means of regulating them.[4] Offenders also evade prosecution by "mixing" legal and illegal conduct.[5] Some countries have even fewer methods in place to address abuses in cyberspace.

Of course, some countries, especially those with totalitarian governments, are approaching the problem of Internet pornography as merely part of what they see as a larger issue of Western influence, political dissent, and information control. By screening out most content, sometimes virtually all foreign Internet sites, and aggressively enforcing restrictive laws, governments in these countries are effectively restricting access to Internet pornography. These countries simply block any possibly questionable site—an approach much simpler than managing a carefully calibrated regulatory scheme. However, the methods in these totalitarian countries provide no useful guidance for countries wishing to address the problem with a scalpel rather than a sledgehammer.

As the country that built and still largely dominates the Internet, the United States should be a leader in modeling solutions for cyberabuse, a standard bearer in showing the world that the rule of law, freedom, and respect for values can be simultaneously balanced, accommodated, and fostered. Unfortunately, the United States has floundered, falling behind other countries in addressing the problem.[6] All but the most limited regulatory efforts in the United States have been poorly conceived, remain out of touch with technology, or have failed to pass constitutional scrutiny.[7]

---

2. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 81–84 (2006); *see also* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005). (proposing that Internet service providers (ISPs) have a limited duty of care to remove or block tortious activities using their services when they have received actual notice of those activities).

3. GOLDSMITH & WU, *supra* note 2, at 81.

4. *Id.* at 82.

5. *Id.* at 83–84 (stating that "mixing" occurs where illegal conduct (e.g., publishing obscene material) is difficult to distinguish from legal conduct (e.g., publishing news, artistic expression, and sexual education), "so that a given business . . . can only be stopped at the expense of giving up things that government and society value highly—like artistic expression and an open environment for speech").

6. For further information on the efforts of countries outside the United States to address indecency online, see Cheryl B. Preston, *Offshore Porn is a Flimsy Excuse* (forthcoming 2008).

7. For an overview of failed federal efforts to regulate online pornography, see Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BYU L. REV. 1417. For a state effort found to be unconstitutional, see the Pennsylvania Solution discussed in Jonathan Zittrain, *Internet Points of*

In 1997, the U.S. Supreme Court struck down the Communications Decency Act (CDA).[8] Congress responded by passing the Child Online Protection Act (COPA) to correct the constitutional defects in the CDA.[9] The Supreme Court found that COPA likely violated the First Amendment because the government had not meet its burden of proof in showing that less restrictive alternatives (especially filters) would be less effective.[10] On remand in *ACLU v. Gonzales*,[11] Judge Reed, for the Eastern District of Pennsylvania, issued a permanent injunction against the enforcement of COPA, ruling that COPA was not narrowly tailored and was not the least restrictive method for enforcing Congress' compelling interest.[12] The treatment of the CDA and COPA in the courts illustrate the struggle to develop regulatory strategies to protect children while maintaining robust Internet access. The United States has been unable to respond appropriately and provide a model for the rest of the globe for an intelligent balance of safety and privacy, adult and child use.

One argument against pushing forward to craft a workable solution is that the borderless nature of the Internet means adopting a U.S. law would be pointless. Indeed, because of often contradictory intra- and inter-country regulatory difficulties, more uniformity and international leadership in Internet regulation is essential. This paper argues that The Internet Corporation for Assigned Names and Numbers (ICANN), the administrator of the domain name system (DNS), may provide some assistance in crafting a global approach these problems. Although ICANN has resisted involvement in enforcement of some kinds of Internet regulations, ICANN and other entities in the DNS that ICANN supervises, known as registrars and registries, and the contractual obligations among those entities, may provide a means of enforcing national laws regulating online conduct.

In Part I, this article first provides a brief background on the history and structure of ICANN and then illustrates that, despite its claims to the contrary,[13] ICANN does now make and implement policy in non-technical areas of Internet governance. This article then examines how ICANN structures and obligations within the DNS have been used to implement those policy objectives. Second, we describe a piece of ICANN's extant policy structure that can be meaningfully engaged in helping countries carry out reasonable pornography regulation. This

---

Control, 44 B.C. L. REV. 653 (2003); Jim Hu, *Court Strikes Down Pennsylvania Porn Law*, CNET NEWS, Sept. 10, 2004, http://news.com.com/Court+strikes+down+Pennsylvania+porn+law/2100-1028_3-5361999. tml. . For the district court's 109 page memorandum opinion, see Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004),*available at* http://www. dt.org/speech/pennwebblock/20040910memorandum.pdf.

8. Reno v. ACLU, 521 U.S. 844 (1997).

9. Ashcroft v. ACLU, 542 U.S. 656, 660 (2004).

10. *Id.* at 666–69, 673.

11. 478 F. Supp. 2d 775 (2007). The case has been appealed to the Third Circuit, Docket Number 07-2539 (filed May 25, 2007).

12. 478 F. Supp. at 778–79.

13. *See infra* notes 33–36 and accompanying text.

approach does not require radical changes in national or global law or Internet structure; instead, it enables governments to enforce existing pornography laws that have been difficult to enforce because of the Internet's borderless nature.

This approach, discussed in Part II, is based on the existing language in ICANN-mandated agreements. We describe how this language, and the even more extensive language adopted by ICANN-authorized registrars, registries and ISPs, establishes the legal basis for carrying out the enforcement of laws regulating the Internet. We then detail how this approach can be implemented in the United States under existing rules on jurisdiction and the reach of injunctions.

I. ICANN CAN AND DOES NOW MAKE POLICY

Because ICANN was formed and enabled through a series of agreements involving the U.S. government and other Internet administrators, rather than by statute, the process took many complex and confusing turns.[14] We include only a brief overview here. Before ICANN's creation, domain name administration was performed by Network Solutions Inc. (NSI), a U.S. government contractor based in Virginia.[15] In February 1998, the U.S. government began privatizing the management of domain names in a proposed regulation commonly known as the "Green Paper."[16] Then, instead of making the Green Paper a final ruling, the administration issued a nonbinding statement of policy known as the "White Paper" in June 1998. The White Paper called for a private entity to contract with the Department of Commerce (DoC) to administer the DNS.[17]

A short time later, the U.S. government announced that ICANN was the entity contemplated in the White Paper. ICANN's relationship with the DoC has been governed by a Memorandum of Understanding, signed November 25, 1998, which has been amended and renewed various times over the years.[18] Although the DoC declared that ICANN should assume certain functions under the White Paper, government contractors such as NSI continued to perform many of these functions without acknowledging ICANN's role. To correct this, in 1999, the

---

14. For a detailed description of this process, see MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 141–208 (2002); A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 50–93 (2002); Jeff Tyson, *How Internet Infrastructure Works: A Hierarchy of Networks*, HOWSTUFFWORKS, http://computer.owstuffworks.com/internet-infrastructure1.htm (last visited Oct. 24, 2007).

15. For descriptions of domain name administration fundamentals, see MUELLER, *supra* note 14, at 30–56; Froomkin, *supra* note 14, at 37–50; Markus Müller, *Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet*, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 709, 713–19 (2005).

16. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA), IMPROVEMENT OF TECHNICAL MANAGEMENT OF INTERNET NAMES AND ADDRESSES, 63 Fed. Reg. 8825 (Feb. 20, 1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm.

17. Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 5, 1998), *available at* http://www.icann.org/general/white-paper-05jun98.htm.

18. *See* International Corporation for Assigned Names and Numbers (ICANN), ICANN's Major Agreements and Related Reports, http://icann.org/general/agreements.htm (last visited Mar. 27, 2008).

DoC, ICANN, and NSI signed a series of three agreements in which the DoC leveraged its power to encourage NSI to acknowledge ICANN and provide ICANN with financial support.[19] On September 20, 2006, ICANN and the U.S. government again renewed their relationship in the form of a Joint Project Agreement (JPA).[20]

ICANN, a not-for-profit organization incorporated in California,[21] oversees the procedures by which domain names are assigned and given access to the system over which electronic signals are sent on the World Wide Web.[22] It administers the DNS, the system that resolves numerical Internet Protocol (IP) addresses from alpha-numeric domain names.[23] ICANN operates the Internet Assigned Numbers Authority (IANA) that "allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet."[24] For example, through the DNS, "192.0.34.163" becomes "www.icann.org."[25] Part of this system involves ICANN supervising registrars who sell domain names, registries who maintain the databases of domain names, and regional Internet registries who allocate IP addresses.[26] ICANN also administers the "root" or "root zone file," which is one of the master lists of all top-level domains (TLDs) and their associated IP addresses.[27]

As the head of the DNS, ICANN has substantial power over the Internet. ICANN has used this authority in the past to institute policies protecting intellectual property rights at the encouragement of the trademark lobby. In addition, ICANN's dispute resolution policy, the Uniform Domain Name Dispute Resolution Policy (UDRP), has had a dramatic impact on domain name disputes and is one of the few (nearly) Internet-wide regulatory policies.

Other aspects of ICANN's governance have not resulted in high profile policies like the UDRP, but still have significant influence on Internet management and regulation. For example, ICANN has authority over various

---

19. *See generally* Froomkin, *supra* note 14, at 89–93.

20. NTIA, JOINT PROJECT AGREEMENT (Sept. 25, 2006), http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/ICANNBoardResolution_09252006.htm.

21. ICANN, Articles of Incorporation of Internet Corporation for Assigned Names and Numbers (Nov. 21, 1998) http://www.icann.org/general/articles.htm.

22. *See* ICANN, ICANN Information, Mar. 26, 2007, http://icann.org/general/; ICANN, Bylaws for Internet Corporation For Assigned Names and Numbers, Sec. 1, Feb. 28, 2006, http://www.icann.org/general/bylaws.htm#II.

23. For further information about the domain name system (DNS) and its administration, see *supra* note 15.

24. Internet Assigned Numbers Authority (IANA), Introducing IANA, http://iana.org/about/ (last visited Apr. 7, 2008).

25. ICANN, Welcome to ICANN, http://icann.org/new.html (last visited Feb. 13, 2008).

26. *See* Charles M. Kozierok, *IP Overview and Key Operational Characteristics*, TCP/IP Guide, http://www.tcpipguide.com/free/t_IPOverviewandKeyOperationalCharacteristics.htm (last visited Dec. 21, 2007) (discussing Internet Protocols (IPs) and their purpose as points of reference); MUELLER, *supra* note 14, at 188 (noting ICANN's "authority over almost all retail domain name registration"); A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, 2003 U. ILL. L. REV. 1, 18–20 (2003) (describing the "hierarchical" structure between ICANN, the registries, and the registrars); *see also infra* notes 87–89 and accompanying text.

27. *See* Froomkin, *supra* note 14, at 43–47, 89–90.

entities in the DNS such as generic top-level domain (gTLD) registrars and registries.[28] It has artificially limited the number of registrars it accredits. ICANN also chooses which companies "win" the ability to act as registries administering the domain names in a TLD.[29] ICANN enters into contracts with these registrars and registries,[30] and through these contracts, it is able to set technical standards for these entities.

ICANN's contracts also cover other non-technical obligations of registrars and registries. For example, ICANN requires registrars to enter into contracts with domain name registrants that require the registrants to submit to jurisdiction both where the domain name holder is domiciled and where the registrar is located.[31] This provision has significant non-technical consequences.[32] In addition, because the provision is uniformly required for all domain name holders registered with ICANN-accredited registrars, it has significant regulatory utility. As a result, a country seeking to regulate illegal conduct on the Internet within its borders may fashion legislation that relies on the uniformity of certain provisions in ICANN's contracts with entities in the DNS.

ICANN maintains that it does not set non-technical policy. The party line is that ICANN merely coordinates the technology and ensures stable virtual architecture. According to Esther Dyson, ICANN "governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the Domain Name System in particular."[33] The DoC originally called ICANN's function "coordination."[34]

However, others claim ICANN is a regulatory institution that wields quasi-governmental power and that engages in policymaking.[35] Some have stated that

---

28. ICANN also has agreements with the registrars and registries of sponsored top-level domains and some country-code top-level domains (ccTLDs), but many of these agreements are substantially different from the agreement with generic top-level domain (gTLD) entities and are not analyzed here.

29. Froomkin & Lemley, *supra* note 26, at 22-25, 52-56 (criticizing ICANN's artificial logjamming of new gTLDs and registries and discussing possible antitrust implications).

30. ICANN has contracts with most but not all registrars or registries around the world; for example, it does not have agreements with most registrars and registries of ccTLDs. *See* ICANN, ccTLD Agreements, June 6, 2007, http://www.icann.org/cctlds/agreements.html. ICANN is supposed to be working toward obtaining agreements with these entities. *See* NTIA, *supra* note 20, at ¶ 5 ("ICANN shall continue its efforts to achieve stable agreements with ccTLD operators.").

31. ICANN, Registrar Accreditation Agreement, § 3.7.7.10, May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm#3.

32. *See infra* notes 90–91 and accompanying text.

33. Letter from Esther Dyson to Ralph Nadar and Jamie Love (June 15, 1999), *quoted in* MUELLER, *supra* note 14, at 8.

34. Management of Internet Domain Names and Addresses, 63 Fed. Reg. 31,741, 31,744 (June 5, 1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm ("Under the Green Paper proposal, the U.S. Government would gradually transfer these coordination functions to the new corporation"); Froomkin, *supra* note 14, at 95.

35. *See* Milton L. Mueller, *Why ICANN Can't*, IEEE SPECTRUM 15, 15 (July 2002); *see also* Froomkin, *supra* note 14, at 94–105; David Post, Governing Cyberspace, June 6, 1999, http://www.icannwatch.org/archive/governing_cyberspace.htm (noting some of ICANN's actions are "already way beyond the realm of technical 'standards-setting'" and involve "global Internet policy").

its mandate from the DoC to administer the DNS is analogous to that of the U.S. Federal Communications Commission (FCC), which few would argue engages only in technical coordination.[36]

Perhaps initially administering the DNS was simply a matter of technical coordination, when all it required was the one-person job of recording all the domain names and numbers in a single notebook. However, when domain name registration exploded under the oversight of NSI in the 1990's, the job quickly became more than technical coordination. An example of this development occurred in July 1995 when NSI became involved in its first trademark lawsuit. To avoid being involved in such suits in the future, NSI issued a "Domain Dispute Resolution Policy Statement" to address disputes regarding domain names and their registration.[37]

ICANN took over various Internet governance functions previously performed by NSI in the late 1990s, and as the Internet has grown, ICANN's policy, gate-keeping, and business-opportunity functions have increased. For example, ICANN caps the cost of registering a domain name.[38] It has taken a policy stand on the demand for domain names by controlling the number of new TLDs.[39] Similarly, ICANN accredits a limited number of registrars, creating competition among prospective and existing registrars in what has become an extremely lucrative business.[40] It also determines which companies receive certain types of economic opportunities, such as being a registry over an existing or new group of domain names.[41]

ICANN prescribes many of the key contractual provisions that registrars must impose on all new applicants for domain names, and ICANN also requires modification of existing contracts to include the provisions.[42] It requires domain name holders to submit to an accelerated arbitration process pursuant to the UDRP to determine the scope of a party's trademark rights.[43] ICANN determines the scope of domain name holders' personal privacy rights by setting policies for what personal information a registrar collects from domain name applicants

---

36. *See, e.g.*, Mueller, *supra* note 35, at 16.

37. MUELLER, *supra* note 14, at 120.

38. *See* Mueller, *supra* note 35, at 16.

39. *See id.* ("ICANN . . . controls the supply of [domain] names by accepting or rejecting applications for top-level domains (.com, .net, and the like)").

40. *See* ICANN, Accreditation Overview, Mar. 26, 2007, http://www.icann.org/registrars/accreditation.htm.

41. *See* ICANN, Registry Services Evaluation Process, Mar. 26, 2007, http://www.icann.org/registries/rsep/.

42. Froomkin, *supra* note 14, at 97.

43. *See infra* text accompanying notes 47–59; *see also* Mueller, *supra* note 35, at 16; Froomkin, *supra* note 14, at 101 (noting that the UDRP "represents a clear policy choice to sacrifice the interest of (some) domain name registrants in favor of (some) trademark registrants for the communal good"); Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 216 (2000) (describing the implementation of the UDRP as "command-and-control regulation").

under ICANN's WHOIS policy.[44] It sets technical standards for the administration of registration databases and the sharing of information among other DNS coordinating bodies. Milton Mueller illustrates that "ICANN's decisions directly affect numerous interest groups: consumers of domain name services, trademark holders, civil liberties advocates, existing registries and their would-be competitors, law-enforcement agencies, would-be censors, and foreign governments."[45] Finally, it has in fact, chosen to become involved, although not effectively, in the issues of adult content on the Internet and methods of protecting children from such content.[46]

Perhaps the most influential interest group for whom ICANN has made policy is trademark holders. Trademark holders were involved in the dialogue that shaped Internet governance almost from the beginning, playing a role in NSI decisions and then becoming central to the creation of ICANN and ICANN's UDRP.[47] NSI created a trademark dispute resolution policy before ICANN was conceived.[48] Trademark holders were present in a series of conferences and workshops that in 1995 and 1996 on Internet administration and coordination. They objected to a proposal known as "draft-postel," which would have added more TLDs. The trademark holders enlisted the U.S. Patent and Trademark Office and the DoC to help them argue that ignoring trademarks in relation to Internet governance would negatively impact commerce.[49]

IBM and AT&T, big businesses heavily invested in Internet development, withheld their support from an alternative proposal to the Green Paper developed by the International Ad-Hoc Committee (IAHC) because of trademark concerns.[50] These companies and others were also key players in bringing together a "dominant coalition" that negotiated what became known as the White Paper,[51] that led to enabling ICANN.

The White Paper authorized the World Intellectual Property Organization (WIPO), "an entity entirely beholden to intellectual property owners,"[52] to propose a policy for handling trademark disputes. Since the time of the IAHC proposals, trademark interests had lobbied for a domain name management that was directly linked to trademark protection, centralizing the policing and

---

44. ICANN, Whois Services, Mar. 26, 2007, http://icann.org/topics/whois-services/; ICANN, Public Participation Page, Whois Information Page, http://public.icann.org/whois (last visited July 5, 2007) ("'Whois' refers to the information that is required whenever anyone registers a domain name . . . .").

45. Mueller, *supra* note 35, at 16.

46. ICANN recently considered and then rejected an application to create a gTLD, .xxx, exclusively for adult content. *See* ICANN, Board Rejects .XXX Domain Application, Mar. 30, 2007, http://www.icann.org/announcements/announcement-30mar07.htm.

47. *See generally* MUELLER, *supra* note 14, at 73–208.

48. *See supra* note 35 and accompanying text.

49. MUELLER, *supra* note 14, at 137–39, 156.

50. *Id.* at 142–46, 154–60, 168–71.

51. *Id.* at 168–75.

52. *Id.* at 190.

enforcement of trademark holders' rights and shifting the transactions costs away from themselves.[53] The trademark interests attempted to implement this objective through WIPO, which initiated a consultation process to gather suggestions on trademark disputes.[54] WIPO's December 1998 interim report attempted to secure the strongest intellectual property protection imaginable.[55] It included, for example, the WHOIS database, which "offered . . . automated and centralized surveillance of registration records" and "offered administrators the leverage for effective and inexpensive enforcement: the withdrawal of the domain name."[56] Based on the strong negative response from civil rights groups, academics, and others, WIPO revised its proposal and submitted a more modest report, but the report still contained a pro-trademark holder bias.[57]

Trademark holders have continued as an influential voice in the development of ICANN's policies. As Michael Palage, the head of the Registrars' Domain Name Supporting Organization (DNSO) Constituency, famously noted, "[t]he trademark lobby must be placated because of its potential ability and inclination to bankrupt new registrars and wreak havoc on their registrant databases."[58] The DoC and ICANN heeded the trademark lobby by making the introduction of new TLDs a low priority relative to other goals. When new TLDs were eventually approved, "sunrise" or "daybreak" procedures accompanied the new TLDs, allowing trademark holders the opportunity to register their names before the public.[59] These procedures illustrate how trademark holders affected the policies of ICANN during its development.

ICANN listened to and incorporated the concerns of trademark and intellectual property owners from the beginning. But its tie to these groups did not end there. Through 1998 and most of 1999, NSI's refusal to recognize ICANN prevented ICANN from receiving revenues from new registrars under its shared registration system, which would have introduced competition in registration by adding additional registrars.[60] Because it did not receive revenues as planned, ICANN had no financial support and went deeply into debt.[61] The benefactors who bailed ICANN out were, of course, the corporate interests who

---

53. *Id.*

54. *Id.*

55. *Id.* at 190–91.

56. *Id.* Among those opposed to the report were "domain name registries, organizations representing the Internet technical community, civil liberties groups, and many individual domain name holders." *Id.*

57. *See id.* at 192–93.

58. Judith Oppenheimer, Beware Slippery Slopes AKA Be Careful What You Wish For . . . http://www.judithoppenheimer.com/pressetc/adentive.html (last visited Mar. 25, 2008) (quoting a remark by Palage at a January 10, 2000 meeting of the Small Business Administration on domain name issues).

59. MUELLER, *supra* note 14, at 193.

60. *Id.* at 194–95.

61. *Id.* at 195.

held the largest stake in ICANN's survival. For instance, MCI loaned ICANN $500,000, and Cisco Systems loaned it $150,000.[62]

In summary, ICANN's policies, especially the UDRP, were the product of input by many economic interest groups, including in particular large corporations with huge economic stakes in protecting their trademarks and intellectual property.[63] Their lobbying efforts are plainly evident in the policies that ICANN developed early on, the objectives the DoC designed it to fulfill, and the path ICANN has pursued since its creation. Many of ICANN's decisions reflect distinct policy choices that protect trademark holders in opposition to the interests of domain name registries, the Internet technical community, civil liberties groups, individual domain name holders, foreign governments, and the public generally.[64] In fact, interest groups representing the general public were clearly missing from the table when these initial policy decisions were made. The general public at that time had little understanding of the Internet, its potential for good and for ill, and although this group has a huge stake in what the Internet becomes and allows, it has none of the economic and lobbying power already entrenched in the ICANN system by well-financed trademark and intellectual property owners.

Because ICANN has been the instrument for maintaining various public policies since its inception, there is no justification for its current argument that it does not make "policy," and that it can't be both socially responsible and economically driven. Given that reality, this paper suggests a possible avenue by which the obligations contained in ICANN's contracts can contribute meaningfully to the enforcement of pornography laws on the Internet.

II. ICANN CAN AND DOES REQUIRE CONTRACT PROVISIONS

ICANN already has in place an elaborate structure of contracts and memorandums of understanding, as well as informal agreements, with many of the actors in the Internet hierarchy. These agreements give ICANN considerable power and also provide a mechanism for uniform Internet regulation of gTLDs. As governments become increasingly concerned about the easy availability of Internet pornography within their boundaries, these contractual obligations and relationships will have increasing importance. In addition, because these contractual obligations suggest ways that court orders can be used to control pornography on the Internet, we will also examine in this section issues of jurisdiction and the enforcement of court orders in Subpart B.

---

62. James Niccolai, *ICANN Survives on Corporate Dole*, INDUSTRY STANDARD, Aug. 20, 1999, *available at* http://thestandard.com/article/0,1902,6037,00.html.

63. MUELLER, *supra* note 14, at 166–67 tbl. 8.1.

64. *See, e.g.*, *supra* note 56 (listing parties who opposed the World Intellectual Property Organization's (WIPO) interim report).

A. Contractual Rights and Duties Deriving from ICANN and its Affiliates

ICANN requires that all accredited registrars incorporate the UDRP by reference into all registration agreements with domain name holders.[65] The UDRP was established by ICANN and has been adopted by all accredited domain name registrars of all gTLDs,[66] and a few domain name registrars of country-code top-level domains (ccTLDs).[67] The UDRP provides that a registrar *will* cancel, transfer, or make other changes to domain name registrations upon receipt of a court order. The relevant provision provides:

> 3. Cancellations, Transfers, and Changes. We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:
>
> . . . .
>
> b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
>
> c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. . . .[68]

The policy is incorporated by reference into the registration agreement between a registrar and a domain name holder.[69] In other words, "we" in the quote above refers to the registrar and "you" refers to the domain name holder. ICANN is not a party to this contract.[70]

---

65. The Registrar Accreditation Agreement between accredited registrars and ICANN provides as follows:

> 3.8 Domain-Name Dispute Resolution. During the Term of this Agreement, Registrar shall have in place a policy and procedures for resolution of disputes concerning Registered Names. Until different policies and procedures are established by ICANN under Section 4, Registrar shall comply with the Uniform Domain Name Dispute Resolution Policy identified on ICANN's website . . . .

ICANN, Registrar Accreditation Agreement, May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm.

66. ICANN, Domain Name Dispute Resolution Policies, Sept. 11, 2007, http://www.icann.org/udrp/ (noting that the UDRP "has been adopted by ICANN-accredited registrars in all gTLDs (.aero, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel).").

67. ICANN, Uniform Domain Name Dispute Resolution Policy, Oct. 24, 1999 http://www.icann.org/dndr/udrp/policy.htm, at Note 2 (noting that the UDRP has been adopted by "certain managers of ccTLDs (e.g., .nu, .tv, .ws).").

68. *Id.* ¶ 3.

69. *Id.* ¶ 1 ("This Uniform Domain Name Dispute Resolution Policy . . . is incorporated by reference into your Registration Agreement . . . .").

70. *Id.* at Note 3 ("The policy is between the registrar (or other registration authority in the case of a country-code top-level domain) and its customer (the domain-name holder or registrant). Thus, the policy uses 'we' and 'our' to refer to the registrar and it uses 'you' and 'your' to refer to the domain-name holder.")

Some might argue that the language of Paragraph 3(b) only applies to trademark disputes. However, when the UDRP is read as a whole, the separation of the arbitration provisions in Paragraph 4 of the policy from the contract requirements in Paragraph 3 makes clear that Paragraph 3 refers to disputes generally. Subparagraph 3(b) provides in plain language that a registrar will cancel, suspend, or transfer a domain name solely upon receipt of an order of a court or tribunal of competent jurisdiction.

Under the UDRP and relevant case law, courts of "competent" jurisdiction include those authorized by a government to adjudicate the claims brought before them.[71] Thus, if a U.S. court finds that material on the web is illegal—for instance, child pornography or unprotected obscenity—the court may issue an order requiring that the material be taken down or that the website be forfeited. When served with this order, the registrar "*will* cancel, transfer or otherwise make changes to domain name registrations."[72]

Other contractual provisions also illustrate that registrars may suspend or transfer a domain name upon receipt of a court order. The following provision in the registrar accreditation agreement between accredited registrars and ICANN requires that the registrar include certain provisions in its registration agreements with registered name holders:

> 3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions:
>
> . . . .
>
> 3.7.7.11 The Registered Name Holder shall agree that its registration of the Registered Name shall be subject to *suspension, cancellation, or transfer* pursuant to any ICANN adopted specification or policy, or pursuant to any registrar or registry procedure not inconsistent with an ICANN adopted specification or policy . . . (2) *for the resolution of disputes concerning the Registered Name.*[73]

These provisions could be read very narrowly so that a dispute over the content of a particular website might not be considered a dispute "concerning the registered name." However, the language equally lends itself to being read more broadly to refer to any dispute that involves the domain name, so that disputes over the content of the site would be included as well.

---

71. *See* Storey v. Cello Holdings, L.L.C., 347 F.3d 370, 380 (2d Cir. 2003) ("As the UDRP provides no definition for 'court of competent jurisdiction' as a term of art, we give the term its plain meaning, namely a court that has jurisdiction to hear the claim brought before it.").

72. *See* ICANN, *supra* note 67, at ¶ 3 (emphasis added).

73. ICANN, Registrar Accreditation Agreement, § 3.7.7.11, May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm#3 (emphasis added).

Similar language appears in the contracts between customers and other parties in the DNS. For instance, *Go Daddy*, a large accredited registrar located in the United States uses a provision very similar to the above language in ICANN's accredited registrar agreement.[74] Another accredited registrar, *000Domain.com*, uses even stronger language regarding power to cancel domain names.[75] Its contract includes the following:

> 16.2 Domain suspension, cancellation or transfer. You acknowledge and agree that your domain registration is subject to suspension, cancellation or transfer (cancellation or transfer collectively referred to as, "Cancellation") . . . (b) *for the resolution of disputes concerning the domain pursuant to an ICANN policy or procedure.* You also agree that 000Domains shall have the right in its *sole discretion to suspend, cancel, transfer or otherwise modify a domain registration . . . after such time as 000Domains receives a properly authenticated order from a court of competent jurisdiction, or arbitration award, requiring the suspension, cancellation, transfer or modification of the domain registration.*
>
> 16.3 Termination. *000Domains reserves the right to suspend, cancel, transfer or modify your domain registration if: . . .* (b) *you use the domain to send Unsolicited Email, in violation of this Agreement or applicable laws*;[76] (c) *you use your domain in connection with unlawful activity*; or (d) you violate this Agreement.[77]

This language gives wide latitude to the registrar to unilaterally suspend or terminate a domain name. Subsection 16.3(c) certainly covers the use of the domain to publish currently illegal content such as obscenity or child pornography.

More importantly, these provisions demonstrate that an accredited registrar can, through its own contract initiative (or in conformity to a contractual

---

74. Go Daddy Software Inc., Go Daddy Domain Registration Agreement, Nov. 1, 2006, http://www.godaddy.com/gdshop/legal_agreements/show_doc.asp?pageid=REG_SA.

> 6. suspension of services; breach of agreement. You agree that, in addition to other events set forth in this agreement, (i) Your ability to use any of the services provided by Go Daddy is subject to cancellation or suspension in the event there is an unresolved breach of this agreement and/or suspension or cancellation is required by any policy now in effect or adopted later by ICANN, and (ii) Your registration of any domain names shall be subject to suspension, cancellation or transfer pursuant to any ICANN adopted specification or policy, or pursuant to any Go Daddy procedure not inconsistent with an ICANN adopted specification or policy, (1) to correct mistakes by Go Daddy or the registry operator in registering any domain name or (2) for the resolution of disputes concerning any domain name.

75. *See* 000Domains.com, Registration Agreement, ¶ 17.2, Nov. 15, 2006, https://secure.registerapi.com/order/register/agreement.php?siteid=35427 [hereinafter 000Domains.com, Registration Agreement].

76. This appears to refer to violations of the CAN-SPAM Act, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701–13; 18 U.S.C. 1001, 1037; 28 U.S.C. § 994; and 47 U.S.C. § 227).

77. 000Domains.com, Registration Agreement, *supra* note 75. (emphasis added).

requirement from ICANN), draft provisions stricter than the current ICANN requirements. Section 16.3(d) of the 000Domains contract permits the registrar to suspend, cancel, or transfer a registrant's domain name if the registrant "violate[s] th[e] Agreement." In addition, the agreement incorporates present and future ICANN and registrar policies by reference.[78]

Using even more aggressive language, another registrar, *Tucows*, reserves the right to act solely upon receiving notice of the filing of a complaint regarding the domain name.[79] The contract provides:

> If Tucows is notified that *a complaint has been filed* with a judicial or administrative body regarding your domain name, Tucows may, at its sole discretion, suspend your ability to use your domain name or to make modifications to your registration records until (i) Tucows is directed to do so by the judicial or administrative body, or (ii) Tucows receives notification by you and the other party contesting your domain that the dispute has been settled. Furthermore, you agree that if you are *subject to litigation regarding your registration or use of your domain name*, Tucows may deposit control of your registration record into the registry of the judicial body by supplying a party with a registrar certificate from us.[80]

In the first sentence, the operative description of the litigation is "regarding your domain name." In the second sentence, that category seems to be broken down further into "litigation regarding your registration or *use of* your domain name," suggesting that the provision is broad enough to govern website content.

This kind of language is currently being used to shut down websites based on content. For instance, the world's largest registrar, *Go Daddy*, recently suspended a website based on the website's content relying on authority from its terms of service agreement, which is an agreement separate from its registration agreement. Its service agreement allows *Go Daddy* to take down a site for any reason.[81] In that case, *MySpace* alleged that thousands of its users' passwords and

---

78. *Id.* ("To complete the registration process, you must acknowledge that you have read, understood, and agree to be bound by . . . any registration rules or policies that are or may be published from time to time by 000Domains, the Internet Corporation for Assigned Names and Numbers ("ICANN") and/or any and all of the registry administrators.").

79. *See* Tucows Reseller Contract, http://resellers.tucows.com/contracts/tld/exhibita (last visited Feb. 13, 2007).

80. *Id.* (emphasis added).

81. *See* Declan McCullagh, *GoDaddy Pulls Security Site After MySpace Complaints*, CNET.com, Jan. 25, 2007, http://news.com.com/2100-1025_3-6153607.html?part=rss&tag=2547-1023_3-0-5&subj=news; Go Daddy, Go Daddy Universal Terms of Service for Go Daddy Software and Services, Feb. 19, 2007, https://www.godaddy.com/gdshop/agreements.asp?ci=291. The relevant language provides:

> As a condition of Your use of Go Daddy 's Software and Services, You agree not to use them for any purpose that is unlawful or prohibited by these terms and conditions, and You agree to comply with any applicable local, state, federal and international laws, government rules or requirements. You agree You will not be entitled to a refund of any

usernames had been archived on *Seclists.org*, and demanded that *Go Daddy* suspend the *Seclists.org* site. *Go Daddy* complied with *MySpace*'s request and, "[t]o protect the *MySpace* users from potentially having private information revealed[,]" suspended the site until the password list had been removed—a duration of approximately seven hours.[82] *Go Daddy* indicated that it frequently removes domain names based on website content, utilizing a "24-hour abuse department that deletes domain names used for spam or child pornography on a daily basis."[83]

The contractual terms discussed in this section illustrate that (1) ICANN has strong bargaining power vis-á-vis registrars and registrants, such that ICANN is able to mandate the use of specific contractual language; (2) the existing language in ICANN-mandated contracts is sufficient to require suspension of a website upon receipt of a court order arising from anti-pornography laws; (3) both ICANN and accredited registrars already contractually notify registrants of the possibility that domain names may be cancelled; and (4) both ICANN and accredited registrars could set standards and enforcement procedures by contract with domain name owners who publish pornography.

While the use of court orders seems straightforward, there are several issues we must explore concerning the efficacy of using court orders to assist in regulating Internet pornography. Clearly, questions of standards and mechanics will arise. In Subpart B, we address some of the practical and administrative issues that relate to the use of court orders to regulate web content, including jurisdiction and the reach of a court order.

B. Jurisdiction and Enforcement Issues

Understanding the contractual rights and duties among players in the DNS provides lawmakers and interest groups with a framework around which to craft legislation to regulate pornographic material the Internet. First, such interested parties should maximize the use of existing legislation that allows a private party or public official to obtain a court order requiring material to be taken off the

---

> fees paid to Go Daddy if, for any reason, Go Daddy takes corrective action with respect to Your improper or illegal use of its Services.
>
> . . .
>
> . . . . Go Daddy reserves the right to review Your use of the Services and to cancel the Services in its sole discretion. *Go Daddy reserves the right to terminate Your access to the Services at any time, without notice, for any reason whatsoever.*
>
> Go Daddy reserves the right to terminate Services if Your usage of the Services results in, or is the subject of, legal action or threatened legal action, against Go Daddy or any of its affiliates or partners, without consideration for whether such legal action or threatened legal action is eventually determined to be with or without merit.

Id. § A.5 (emphasis added).

82. McCullagh, *supra* note 81 (quoting Go Daddy general counsel Christine Jones).

83. *Id.*

web. Interested parties should also maximize the use of legislation that allows a domain name or distribution scheme to be forfeited when it is used to violate law.

In the United States, statutes following this model, which permit the disabling of the means used to carry out illegal activity, already exist in various contexts that could be compared to the regulation of pornography. For instance, under the Digital Millennium Copyright Act (DMCA), courts may impound any device or product related to the copyright violation, and grant injunctions or "order remedial modification or destruction of a violating device or product."[84] Similarly, the 2003 Controlling the Assault of Non-Solicited Pornography and Marketing (CANSPAM) Act provides that an offender forfeits "any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense."[85]

In countries without such legislation aimed directly at online pornography, the political push should be to convince legislatures to adopt provisions that proscribe certain forms of pornography and explicitly or implicitly empower a court, or other tribunal, to issue a cease-and-desist type order. Legislation should be drafted to provide, among other remedies, the express power of a court to issue an order for a site to be taken down if it is being used to publish illegal pornographic material.

Unfortunately, because of the borderless nature of the Internet, lawsuits involving Internet actors may not be as simple as a lawsuit against a hard-copy, geographically-bounded pornographer. In drafting new legislation, proponents should be aware of two potential problems: (1) obtaining jurisdiction over domain names and domain name holders, and (2) establishing the injunctive reach of a court's order. What follows is a discussion of these two issues under U.S. law. We do not undertake here to discuss the jurisdiction regimes in other countries or international choice of law rules.

1. Jurisdiction

For a court to hear a case, make a binding ruling, and then issue an order enjoining the continued availability of a website, the court must have jurisdiction over the person or the thing—the person who controls the website or the site itself. Generally, these will be respectively a domain name holder and the domain name itself. The preferred basis for jurisdiction is *in personam*,[86] and we address it first, followed by *in rem* jurisdiction.

---

84. 17 U.S.C. § 1203 (2000).

85. 18 U.S.C. § 1037.

86. We note that federal courts begin analyzing personal jurisdiction over out-of-state defendants by looking to the state long-arm statute of the state where the court sits. *See* Fed. R. Civ. P. 4(k)(1)(A). Many states, although not all states, attempt to assert personal jurisdiction to the fullest extent allowed by due process. *See* 4 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 1068 (3d ed. 2002). We will only analyze the constitutional limitations on personal jurisdiction here and leave a more complete analysis of long-arm statutes to a future article.

Under U.S. law, the personal jurisdictional issues are slightly different for three classes of domain name holders: domestic registrants, foreign registrants registered with a U.S.-based registrar, and foreign registrants registered with a foreign-based registrar. It is important to note the difference between registrars and registries. Registrars are entities that sell domain names retail to the public.[87] Registries, on the other hand, include entities that administer a TLD.[88] A distinct type of registry is a regional internet registry that assigns domain names to numbers. Collectively, these entities are responsible for the allocation, registration, and administration of IP numbers within a specific geographic location.[89] Regional Internet registries focus on technical aspects of coordinating IP address allocation.

a. Domestic Registrants

For purposes of jurisdiction, the first category of domain name registrants (or owners) is those domiciled in the United States. These domain name holders are subject to *in personam* jurisdiction in the state and federal courts in the districts where they are domiciled. They are also subject to jurisdiction in the state or federal court of every state in which they have minimum contacts that satisfy due process.[90]

b. Foreign Registrants Registered With a Domestic Registrar

The second category of domain name holders is foreign entities who register with a U.S.-based registrar. The ICANN Registrar Accreditation Agreement requires that a registrar compel a domain name holder to submit to jurisdiction both where the registered name holder is domiciled and where the registrar is located.[91] A literal reading of this agreement subjects any domain name holder, whether domiciled in the United States or not, who registers its domain name through a U.S.-based registrar, to jurisdiction where the registrar is located. Even

87. For a list of registrars accredited by ICANN, see ICANN, ICANN-Accredited Registrars, http://www.icann.org/registrars/accredited-list.html (last visited Mar. 27, 2008).

88. For a list of registries, see ICANN, Registry Listing, http://www.icann.org/registries/listing. html (last visited Mar. 27, 2008).

89. Early on it was decided that the management of domain names should be separate from the management of IP numbers. Daniel Karrenberg et al., *Development of the Regional Internet Registry System*, 4 INTERNET PROTOCOL J. 17 (Dec. 2001), *available at* http://www.cisco.com/ web/about/ac123/ac147/archived _issues/ipj_4-4/regional_internet_registries.html.

90. *See* International Shoe Co. v. Washington, 326 U.S. 310 (1945), and its progeny; *see also* GEOFFREY C. HAZARD ET AL., PLEADING AND PROCEDURE 163–346 (9th ed. 2005).

91. ICANN, Registrar Accreditation Agreement, § 3.7.7.10, May 17, 2001, http://www.icann.org/ registrars/ra-agreement-17may01.htm#3. The provision provides in full: "3.7.7.10. For the adjudication of disputes concerning or arising from use of the Registered Name, the Registered Name Holder shall submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) of the Registered Name Holder's domicile and (2) where Registrar is located." *Id.*

under a narrow reading of the agreement, foreign registrants who have minimum contacts with the United States would also be subject to jurisdiction.[92]

c. *Foreign Registrants of a Domain Name Registered With a Foreign Registrar*

A third category is domain name holders who are foreign registrants who register their domain names through foreign registrars. Normally, U.S. courts are unable to exercise jurisdiction over these foreign registrants because they do not have sufficient minimum contacts here. However, U.S. courts could exercise jurisdiction over foreign registrants of a domain name in a gTLD administered in the United States if Congress passed a statute with a jurisdictional scheme similar to the Anticybersquatting Consumer Protection Act (ACPA).[93] Alternatively, U.S. courts may exercise jurisdiction over such registrants without new legislation through an *in rem* civil forfeiture action. We next discuss the ACPA scheme and then the existing common law options.

(1) *In rem* jurisdiction under the ACPA. The ACPA provides trademark holders with civil remedies against defendants who obtain domain names in "bad faith."[94] Although the ACPA is a trademark statute, it provides a helpful framework for conceptualizing the jurisdictional issues regarding other violations of law involving domain names.

Under certain conditions, the ACPA allows a trademark holder to file an *in rem* civil action against an infringing website domain name operated by a foreign registrant in the jurisdiction where the "domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located."[95] Although the trademark holder cannot ordinarily reach foreign registrants using a foreign registrar and registry, § 1125(d)(2)(A) of the ACPA provides that the trademark holder may file the *in rem* action in the jurisdiction where the registrar or registry is located when the trademark holder is not able to obtain personal jurisdiction over the domain name holder or is unable to find the holder for service of process, upon a showing of due diligence by sending notice by e-mail or by posting notice of the action.[96] In practice, this provision permits a

92. This analysis would likely proceed under the *Zippo* sliding scale test. *See* Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997); *see also* C. Douglas Floyd & Shima Baradaran-Robison, *Toward a Unified Test of Personal Jurisdiction in an Era of Widely Diffused Wrongs: The Relevance of Purpose and Effects*, 81 IND. L.J. 601, 613–14 (2006) (describing the test and listing the circuits which have expressed approval for or applied the test).

93. 15 U.S.C. § 1125(d) (2006).

94. 15 U.S.C. § 1125(d)(1)(A)(i). "Cybersquatting is the Internet version of a land grab. Cybersquatters register well-known brand names as Internet domain names in order to force the rightful owners of the marks to pay for the right to engage in electronic commerce under their own name." Interstellar Starship Serv., Ltd. v. Epix, Inc., 304 F.3d 936, 946 (9th Cir. 2002) (citing Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 267 (4th Cir.2001)).

95. 15 U.S.C. § 1125(d)(2)(A).

96. *Id.*

U.S. court to obtain jurisdiction over an infringing website when foreign domain name holders using foreign registrars are unavailable for service of process. Since almost all unsponsored[97] gTLDs have their headquarters or an office in the United States, nearly all registrants of domain names in gTLDs are subject to the ACPA.[98] Passing legislation with an approach similar to the ACPA which addresses online pornography would simplify many jurisdiction problems.

(2) *In rem* jurisdiction in a forfeiture action. The online pornography problem may currently be addressed through existing common law *in rem* jurisdiction and forfeiture.[99] For instance, under U.S. obscenity[100] law, "any property, real or personal, used or intended to be used to commit or to promote the commission of [an] offense" involving obscene material is subject to criminal and civil forfeiture.[101] Such a seizure action requires a warrant based on a showing of

---

97. Sponsored top-level domains are more restrictive than other top-level domains because they require being a member of a specified group or organization. *See* ICANN, ICANN Top-Level Domains, Mar. 26, 2007, http://www.icann.org/tlds/.

98. The following table shows where the registries of the unsponsored gTLDs are located as of May 2007.

Registry	Top-Level Domain	Location
NeuLevel	.biz	Sterling, VA
VeriSign	.com	Mountain View, CA
Afilias	.info	Dublin, Ireland; Offices in Philadelphia, PA
IANA .int Domain Registry	.int	Marina del Rey, CA
Global Name Registry	.name	London, United Kingdom
VeriSign	.net	Mountain View, CA
Public Interest Registry (PIR)	.org	Reston, VA
RegistryPro, LTD	.pro	Chicago, IL

ICANN, Registry Listing, http://www.icann.org/registries/listing.html (last visited Mar. 27, 2008); *see also* Afilias, About Afilias, Jan. 14, 2005, http://www.afilias.info/about_afilias/; Neulevel, Contact Us, http://www.neulevel.biz/neulevel/contact_us/index.html (last visited Feb. 13, 2007); VeriSign, About VeriSign, Contact VeriSign, http://www.verisign.com/verisign-inc/verisign-contact-information/index.html (last visited June 15, 2007).

99. *See* Porsche Cars N. Am., Inc. v. Porsche.net, 302 F.3d 248, 260–62 (4th Cir. 2002) (holding that 28 U.S.C. § 1655, a lien enforcement statute against absent defendants, does not provide jurisdiction for transfer of domain names in a trademark dilution action).

100. Obscenity under U.S. law is a limited category of hard-core pornography that falls within the definition set forth in *Miller v. California*, and exists where

> [T]he average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; . . . the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and . . . the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

413 U.S. 15, 24 (1973) (citations and internal quotation marks omitted).

101. 18 U.S.C. § 1467(a), (c) (2000). The government uses civil forfeiture more often because of the lower burden of proof required and because the offending property may be seized without the full procedural requirements entailed in a criminal charge or conviction. *See* United States v. One 1982 Chevrolet Crew-Cab

probable cause, evidence of the property's involvement (usually as a tool or instrumentality in the commission of a crime involving obscenity), and a finding that the material is obscene under U.S. law.[102]

Such an *in rem* civil forfeiture action requires that the property have a situs within the United States.[103] Courts interpreting the ACPA have held that Congress intended for domain names to be treated as property and that their situs is in the location of the registrar or registry that registered or assigned the domain name.[104] In a U.S. federal obscenity case, where there is no statutory statement of situs such as in the ACPA, the common law would reach a similar conclusion since the registrars or registries are the entities who control domain names.[105]

Thus, it may be possible for a U.S. court to assert *in rem* jurisdiction based on civil and criminal forfeiture over a domain name controlled by a registrar or registry within its district without any analysis of whether the registrant's minimum contacts with the forum satisfy the requirements of personal jurisdiction.[106] Clearly, this question warrants more complete analysis than we have room for here; we only provide a brief summary of the common law.

Our conclusion regarding *in rem* jurisdiction and forfeiture follows from the continuing viability of the territoriality framework in *Pennoyer v. Neff*,[107] recently reaffirmed in *Burnham v. Superior Court*.[108] In *Burnham*, the U.S. Supreme Court held that "jurisdiction based on physical presence alone constitutes due process because it is one of the continuing traditions of our legal system that define the due process standard of 'traditional notions of fair play and substantial justice.'"[109]

However, U.S, Supreme Court jurisprudence may require that, in the context of *in rem* proceedings, a party must still satisfy the minimum contacts analysis

---

Truck VIN 1GCHK33M9C143129, 810 F.2d 178, 183 (8th Cir. 1987) ("[T]he full panoply of constitutional protections afforded criminal defendants is not available in the context of such forfeiture proceedings.") (citation omitted); *see also* Sharon Finegan, *The False Claims Act and Corporate Criminal Liability:* Qui Tam *Actions, Corporate Integrity Agreements and the Overlap of Criminal and Civil Law*, 111 PENN ST. L. REV. 625, 635–36 (2007).

102. Bennis v. Michigan, 516 U.S. 442, 460 (1996) (Stevens, J., dissenting) (describing the civil forfeiture category of "tools or instrumentalities . . . used in the commission of a crime").

103. *See* Thomas R. Lee, In Rem *Jurisdiction in Cyberspace*, 75 WASH. L. REV. 97, 126 & n.154 (2000).

104. 15 U.S.C. § 1125(d)(2)(A); Porsche Cars N. Am., Inc. v. Porsche.Net, 302 F.3d 248 (4th Cir. 2002) (upholding the constitutionality of the Anticybersquatting Consumer Protection Act (ACPA)'s *in rem* jurisdictional provisions). *But see* Catherine T. Struve & R. Polk Wagner, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 17 BERKELEY TECH. L.J. 989 (2002) (arguing that in no cases of foreign cybersquatting would the *in rem* provision of the ACPA be both applicable and constitutional). *See generally* EUGENE F. SCOLES ET AL., CONFLICT OF LAWS 302–05 (4th ed. 2004).

105. *See* Lee, *supra* note 103, at 126–37 (arguing that domain names have their situs where the registrar or registry controlling the property is located).

106. *See* Shaffer v. Heitner, 433 U.S. 186, 211 n.37 (1977).

107. 95 U.S. 714 (1877).

108. 495 U.S. 604 (1990).

109. *Id.* at 619; *see also* 4 CHARLES ALAN WRIGHT & ARTHUR MILLER, FEDERAL PRACTICE AND PROCEDURE § 1073 (2d ed. 1987 & Supp. 1999); Lee, *supra* note 103, at 137–41.

applicable to *in personam* proceedings.[110] But even so, the minimum contacts test is not a serious hurdle. Foreign registrants registering a name in a gTLD with a U.S. based registry purposefully avail themselves of the laws and protections of a U.S. jurisdiction, thus satisfying the "purposeful availment" test.[111] Moreover, this "purposeful availment" may not even be required. Many commentators suggest that personal jurisdiction may be based on objective analyses of effects in the United States rather than a subjective analysis of "purposeful availment."[112]

This section illustrates that the existing common law, as well as a statute following the jurisdictional framework of the ACPA, would permit either an aggrieved party or the U.S. government to bring an *in rem* action against a domain name, whether held by a foreign or domestic holder, as long as the

---

110. *See Shaffer*, 433 U.S. at 212 ("[A]ll assertions of state-court jurisdiction must be evaluated according to the standards set forth in *International Shoe* and its progeny."). Justice Scalia in *Burnham* acknowledged that the approach in *Burnham* departed from this statement in *Shaffer*, but also noted that this statement was dicta. *See* Lee, *supra* note 104, at 139. Fewer contacts may be required to establish *in rem* jurisdiction because of the limited relief available to *in rem* plaintiffs. *See* Adam M. Greenfield, *Reviving the Distinction Between* In Rem *and* In Personam *Jurisdiction by way of the Anti-Cybersquatting Consumer Protection Act*, 35 AIPLA Q.J. 29, 64–66 (2007).

111. *See* Lee, *supra* note 103, at 143. A broader argument of "purposeful availment" that allows sovereign states to exercise jurisdiction over foreign defendants is based on geolocation capabilities and interactivity. Geolocation technology allows online actors to "match an individual user's [IP] address . . . to a geographical location." Calson Analytics, Security & InfoCrime Guide: Geolocation, July, 2005, http://www.caslon.com.au/securityguide15.htm (last visited Mar. 27, 2008). Similarly, geolocation filtering permits an online publisher to vary or restrict the content of her website based on a users' geographical location. *See* Wayne Madsen, *Internet Censorship: The Warning Signs Were Not Hidden*, INFOWARS, Dec. 9, 2005, *available at* http://www.prisonplanet.com/articles/december2005/091205nothidden.htm. Professor Reidenberg concludes that this technology "mean[s] that Internet activity is 'purposefully availing' throughout the Internet whenever content is posted without geolocation filtering." Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1956 (2005). Further, "[t]echnological innovation that enhances interactivity also shifts the burden from demonstrating that a jurisdiction was targeted to showing that reasonable efforts were made to avoid contact with the jurisdiction." *Id.* at 1962.

112. *See* Floyd & Baradaran-Robison, *supra* note 92 at 604 (arguing "for a unified test for personal jurisdiction based on an objective evaluation of the defendant's activities with regard to the forum state"); Wendy Perdue, *Aliens, the Internet, and "Purposeful Availment": A Reassessment of Fifth Amendment Limits on Personal Jurisdiction*, 98 NW. U. L. REV. 455 (2004) (arguing that the limits under the Fifth Amendment are different from those under the Fourteenth Amendment based on a difference in the limitations on sovereign authority in the two clauses); *see also* Reidenberg, *supra* note 111, at 1955, (listing cases that "have looked to online targeting and to deleterious effects within the forum to determine if personal jurisdiction is appropriate"); Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. REV. 323, 332–47 (2003). Courts are also using an effects jurisdictional analysis in other areas of law such as security regulation. *See, e.g.*, Consol. Gold Fields PLC v. Minorco, S.A., 871 F.2d 252, 255, 261–64 (2d Cir. 1989), *amended by* 890 F.2d 569 (2d Cir. 1989) (applying "effects" to conclude under federal securities laws that a tender offer of securities by foreign entities had "sufficient effects within the United States" to permit the district court's exercise of subject-matter jurisdiction over the parties) (citing Schoenbaum v. Firstbrook, 405 F.2d 200 (2d Cir. 1968), *reh'g on other grounds*, 405 F.2d 215 (in banc), *cert. denied*, 395 U.S. 906 (1969); Bersch v. Drexel Firestone, Inc., 519 F.2d 974, 991 (2d Cir. 1975), *cert. denied*, 423 U.S. 1018 (1975); RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1)(c) (1987)) (citations omitted).

Internationally, courts are relying on an effects analysis as well. *See, e.g.*, Dow Jones & Co. v. Gutnick (2002) 210 C.L.R. 575 [Austl.], *available at* http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html (Australia); Richardson v. Schwarzenegger, 2004 EWHC 2422 (Q.B. Oct. 29, 2004), *available at* http://portal.nasstar.com/75/files/Richardson-v-Schwarzenegger%20QBD%2029%20Oct%202004.pdf.

foreign domain name holder uses either a domestic registrar or (almost) any gTLD. The reach of this jurisdiction extends to all websites using .biz, .com, .info, .int, .name, .net, .org, or .pro.[113] However, this approach would not permit jurisdiction in the United States over two of the five largest ccTLDs, .uk and .de,[114] and these domain holders would not be subject to suit in the United States unless they used a U.S. registrar or otherwise had contacts with the United States. If support for pornography regulation and *in rem* jurisdiction were to be garnered in England and Germany, most of the world's Internet traffic would be subject to the take down order of a court with *in rem* jurisdiction.

2. *Injunctive Reach*

Once a court has jurisdiction over the domain name registrant, whether foreign or domestic, the court must still issue an order that will be effective to reach the registrar or registrant with the contractual obligations discussed above in Part II.A. A U.S. federal court's ability to enforce an injunction is informed by Federal Rules of Civil Procedure (FRCP) § 65(d). In this section, we will first discuss the injunction mechanism generally and then examine injunctive reach as it relates to four types of entities involved in providing and regulating domain names on the Internet—registrars, registries, regional Internet registries, and entities involved with ccTLDs.

a. General Injunctive Reach

Section 65(d) of the FRCP provides that an order granting an injunction "binds only the following who receive actual notice of it by personal service or otherwise . . . (A) the parties; (B) the parties' officers, agents, servants, employees, and attorneys; and (C) other persons who are in active concert or participation with anyone described [above]."[115] Thus, the general rule is that nonparties are not usually bound by injunctions. However, U.S. courts have held that "a significant exception occurs where a nonparty has actual notice of a restraining order and is in active concert or participation with a party or his privy."[116] This "active concert or participation" language has been interpreted to include "situations where a nonparty with actual notice aids or abets a named

113. *See supra* note 98.

114. VeriSign, *The VeriSign Domain Report*, 3 DOMAIN NAME INDUSTRY BRIEF 1, 2 (Nov. 2006), *available at* http://www.verisign.com/static/040029.pdf ("In terms of total registrations, the five largest TLDs are .com, the German ccTLD (.de), .net, the British ccTLD (.uk) and .org.").

115. Fed. R. Civ. Proc. 65(d)(2); *see also* Ronald I. Mirvis, Annotation, *Who, Under Rule 65(d) of Federal Rules of Civil Procedure, are Persons "in Active Concert or Participation" with Parties to Action so as to be Bound by Order Granting Injunction*, 61 A.L.R. FED. 482 (1983).

116. Reliance Ins. Co. v. Mast Constr. Co. 84 F.3d 372, 374, 377 (10th Cir. 1996); *see also* Goya Foods, Inc. v. Wallack Management Co., 290 F.3d 63 (1st Cir. 2002); Mirvis, *supra* note 115, at 482 § 6[a] (collecting cases).

defendant or his privy in violating the order."[117] For example, if a bank has actual notice of an order prohibiting all financial institutions with actual notice of the order from permitting a corporate officer to withdraw funds, but nonetheless allows withdrawals, the bank has aided and abetted the officer under this rule.[118]

Similarly, a registrar may not be a party to litigation over a website's content. Nevertheless, even if the registrar is a nonparty, a court's injunctive power vis-à-vis the registrar is informed by this "active concert or participation" analysis. Thus, a registrar or registry with actual notice of an injunction served on a party to the action would be required to affirmatively enforce the injunction by taking down a domain name or web site.

b. Injunctions Ordering Action by Registrars

In the trademark context, at least one court has found that its injunctive power reaches domestic non-party registrars based on FRCP § 65(d)'s "active concert or participation" language and based on the registrar's contractual obligation to enforce court orders.[119] In a case brought in the U.S. District Court for the Eastern District of Pennsylvania, *Worldsport Networks Ltd. v. ArtInternet S.A.*, a French company admitted to infringing on an Irish corporation's trademark by using the domain name "worldsport.com."[120] The court noted that, since the parties stipulated that the plaintiff's trademark rights were violated, the defendants should be enjoined from future violation.[121] As the defendants "committed these violations in part through the registration and naming of their website," the registrar Network Solutions, Inc. (NSI) "acted in concert with Defendants in violating Plaintiff's trademark rights."[122] The court held that it possessed authority to order NSI to transfer registration of the domain name from the defendants to the plaintiff, even though NSI acted "unwittingly and without culpability."[123]

Critics of this expanded view argue that this reasoning may be dicta because NSI did not object to the injunction and had a policy which required it to obey a court's final order without being made a party to the litigation.[124] NSI had, in fact,

---

117. *Reliance*, 84 F.3d at 377.

118. *Id.*

119. Worldsport Networks Ltd. v. ArtInternet, S.A., No. CIV. A. 99-CV-0616, 1999 WL 269719, at *1 (E.D. Pa. Apr. 28, 1999). This case is unpublished, but it is a useful source of analysis on this point.

120. *Id.*

121. *See id.* at *3.

122. *Id.*

123. *Id.*

124. *See id.* at *1–*3 (describing these provisions of NSI's Domain Name Dispute Policy as providing that "when presented with proof of a valid trademark and proof that one of its customers has breached this warranty of non-infringement, it will respect the rights of trademark holders and place the disputed domain name on 'hold' status [and] that NSI will abide by all temporary and final Court Orders directing the disposition of a domain name without being named as a party to the litigation").

reminded the plaintiff of that policy.[125] In addition, after the court concluded that NSI's role as registrar was sufficient to be considered "in active concert or participation" with the infringing defendants, the court noted that "NSI has consented to this exercise of the Court's authority."[126]

Whether the court's FRCP § 65(d) analysis is dicta or not, both readings of the case are interesting here. NSI's Domain Name Dispute Policy, controlling at the time of this case, indicated that it would obey a court order without being made a party to the litigation; this policy is similar if not identical to ICANN's current requirement that registrars cancel a registration upon receipt of a court order directing it to do so.[127] Thus, even if the language quoted above is dicta, the existing ICANN contracts provide the same alternate basis for relief as that relied upon in *Worldsport*.

Requiring "innocent" registrars by injunction to suspend domain names for offending web content is not dissimilar to requiring "innocent" registrars to suspend domain names used by publishers of other offending content. The *Worldsport* court reasoned that an injunction requiring registrars to transfer a domain name is authorized by FRCP § 65(d) and is also supported by the Lanham Act,[128] which "recognizes that even newspapers, magazines and periodicals, as well as printers, may be enjoined from innocent infringement of another's mark as to future publication."[129] An injunction requiring a registrar to suspend a domain name that hosts obscene content under U.S. obscenity law would also be covered by FRCP § 65(d). And, similar to the Lanham Act, federal obscenity law allows the enjoining of publishers and printers from future infringement and also permits the civil and criminal forfeiture of "any property, real or personal, used or intended to be used to commit or to promote the commission of [an] offense" involving obscene material.[130] If the United States were to adopt a measure proscribing the publishing of material harmful to minors[131]—including obscenity, child pornography, and pornography that does not satisfy the *Miller* obscenity test[132]—jurisdiction and the mechanisms for enforcement of injunctions to remove such content, even if published overseas, are already largely available.

Furthermore, in the Internet pornography context, an injunction may be honored by a registrar without the necessity of resorting to the "active concert or participation" exception for nonparties. Section 230 of the Communications

125. *See id.* at *1–*2.

126. *Id.*

127. *See supra* Part II.A.

128. 15 U.S.C. § 1051 (2000).

129. *See* 15 U.S.C. § 1114(2)(A); *Worldsport Networks Ltd.* 1999 WL 269719, at *3; Coca-Cola Co. v. Gemini Rising, Inc., 346 F. Supp. 1183, 1193 (E.D.N.Y. 1972).

130. 18 U.S.C. § 1467(a), (c).

131. For an example of proposed regulation, see Cheryl B. Preston, *Making a Family-friendly Internet a Reality: The Internet Community Ports Act*, 2007 BYU L. REV. 1471.

132. *See supra*, note 100.

Decency Act,[133] upheld by the Supreme Court, contains a provision which addresses a similar issue.[134] Section 230 protects a "provider or user" of an "interactive computer service"[135]—such as a registrar, registry, or ISP—from liability for actions taken in good faith to "restrict access to or availability of material that [it considers] to be . . . objectionable" even if the material is constitutionally protected.[136] Therefore, under this provision, a registrar that restricts access to the objectionable material by suspending a domain name in good faith compliance with a court order is not liable to the domain name holder. Although this provision does not force a registrar to act, the protection from liability for suspending or canceling a domain name may encourage the registrar to take down a site subject to court action without being legally required to do so.[137]

c. *Injunctions Ordering Action by Registries*

Another approach to this problem would be to duplicate, in an anti-pornography law, the statutory approach in the ACPA discussed above. The ACPA allows the filing of an *in rem* action "in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located" under various conditions.[138] Legislation that enforces pornography standards and that parallels the ACPA would allow for the suspension of offending domain names through court orders directed at registries (the entities in charge of TLDs), not just

---

133. 47 U.S.C. § 230.

134. Reno v. ACLU, 521 U.S. 844, 861–64 (1997) (holding unconstitutional §§ 223(a)(1) and 223(d) of the Communications Decency Act under the First Amendment, but upholding other provisions of the Act including § 230).

135. Section 230 defines "interactive computer service" as follows: "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).

136. 47 U.S.C. § 230(c); Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

137. Executive action is another method in which a domestic registrar may be required to suspend or cancel a foreign registrant's domain name. *See* Adam Liptak, *A Wave of the Watch List, and Speech Disappears*, N.Y. TIMES, Mar. 4, 2008, *available at* http://www.nytimes.com/2008/03/04/us/04bar.html. The Office of Foreign Assets Control (OFAC) of the U.S. Treasury Department maintains a list, known as the Specially Designated Nationals (SDN) list, listing individuals and organizations that U.S. citizens and permanent residents are prohibited from doing business with and whose assets are blocked. *See* U.S. Treasury—Office of Foreign Assets Control, Frequently Asked Questions and Answers, http://www.treas.gov/offices/enforcement/ofac/faq/answer.shtml#17 (last visited Mar. 27, 2008). The websites were frozen because the travel agency owning the website was identified as a Cuban national and U.S. companies must freeze all governmental and private Cuban assets. *See* U.S. State Department, Treasury Dept. Identifies Cuban Travel Agency Targeting U.S. Tourists, Dec. 8, 2004, http://usinfo.state.gov/wh/Archive/2006/Dec/08-868923.html; *See also* OFFICE OF FOREIGN ASSETS CONTROL, CUBA: WHAT YOU NEED TO KNOW ABOUT THE U.S. EMBARGO: AN OVERVIEW OF THE CUBAN ASSETS CONTROL REGULATIONS—TITLE 31 PART 515 OF THE U.S. CODE OF FEDERAL REGULATIONS 1–2 (2004), http://www.treas.gov/offices/enforcement/ofac/programs/cuba/cuba.pdf.

138. 15 U.S.C. § 1125(d)(2)(A).

registrars (the entities that sell domain names). By this method a foreign domain name holder, registered through a foreign registrar, may still be subject to a U.S. court's injunction when using a registry headquartered in the United States.[139]

A number of courts have upheld this application of the ACPA to registries as well as registrars. For example, in *Globalsantafe Corporation v. Globalsantafe.com,* the Eastern District of Virginia held that the remedy of suspending the domain name of a foreign registrant through a foreign registrar was appropriate under the ACPA.[140] In *Globalsantafe,* a trademark owner brought an infringement action under the ACPA against an alleged cybersquatter located in Korea.[141] The district court had previously ordered a Korean registrar, Hangang, and VeriSign Global Registry Services (VeriSign) to transfer the contested domain name. A Korean court issued an injunction prohibiting Hangang from transferring the name. The trademark owner then moved to amend the order to direct VeriSign to cancel the domain name until it could be transferred under Korean law.[142]

The Eastern District of Virginia determined first that both cancellation and transfer of the domain name are authorized remedies under ACPA and then analyzed the appropriateness of the requested relief given the specific facts of the case.[143] The court appeared cautious in extending its reach beyond the Korean registrar to a higher level in the DNS, the U.S. based registry VeriSign, even though the ACPA's language refers to both the registrar and the registry.[144] The court considered the expansive jurisdictional reach of the ACPA, noting that VeriSign headquarters were in the court's district and the popularity of the .com and .net TLD names administered by VeriSign meant that this court would likely be asked to assert jurisdiction over domain names owned all over the world.[145] Nonetheless, the court asserted jurisdiction.

---

139. *See supra* note 98.

140. 250 F. Supp. 2d 610, 617 (E.D. Va. 2003).

141. *Id.* at 612–13.

142. *Id.* at 613–14.

143. *Id.* at 617–24.

144. *See, e.g.*, 15 U.S.C. § 1125(d)(2)(A) (2006) (allowing filing of an *in rem* action "in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located").

145. *Globalsantafe*, 250 F. Supp. 2d at 623. The court noted that this aggressive assertion of jurisdiction might cause segmentation of the DNS or the use of ccTLDs, which would impede enforcement of U.S. trademark law on the Internet. *Id.* at 623–24.

Perhaps due to these concerns, the court discussed three possible methods of canceling the domain name. First, the registrar could use a delete command that would direct the registry to delete the information from the Registry Database and the top-level domain zone file. *Id.* at 617, 620–21. Second, the registry could unilaterally disable the domain name. This would put the domain name on hold and make it inactive. Third, the registry could delete the registration information and remove the domain name from the top-level domain zone file upon court order. *Id.* at 617–18, 620–22. These methods involve different kinds of actions and degrees of intrusiveness.

In the *Globalsantafe* case, VeriSign resisted an order requiring the last method because such an order would cause VeriSign to "violate its contracts with the registrar and with ICANN and to interfere with the

The *Globalsantafe* opinion is significant, first, because it shows that a court will extend its jurisdictional and enforcement reach up the DNS hierarchy to registries even when doing so subjects a large number of domain names held by foreign registrants through foreign registrars to jurisdiction in U.S. courts. This decision therefore subjects nearly all registrants of gTLDs to jurisdiction in the United States even though they have contracted with a foreign registrar, because the registries are located in the United States.[146]

Second, the decision disregards the barriers that ICANN's governance structure has tried to develop to isolate certain functions, here registry functions, at specific levels of the governance hierarchy.[147] Third, the decision shows that a U.S. court may require registries located in the United States to unilaterally delete and even unilaterally transfer[148] domain name registrations in the face of resistant foreign registrars and, more significantly, in the face of a foreign court's injunction not to transfer the domain name.

Some criticize the *Globalsantafe* decision because it fails to take account of the added complexity resulting from the diversity of the parties and the conflicting courts involved.[149] The only reason the *Globalsantafe* court engaged in an international-comity analysis instead of a full choice-of-law analysis was

---

registrar-registrant contract" by "acting as a registrar" as prohibited by VeriSign's contract with ICANN. *Id.* at 622. The court was unconvinced by this argument because it was not clear that transferring or canceling a domain name in response to a court order would violate the contract language. *Id.* Second, VeriSign might no longer be bound by a contract with the registrar, Hangang, when the registrar had breached its duties under the contract. Third, these contracts do not limit the remedies available under federal law. *Id.* at 622–23. The court reasoned that all three methods were appropriate under the ACPA, but that the least intrusive method in this case was to order VeriSign to disable the domain name. *Id.* at 623, 626–27. The first method was not available since the Korean registrar Hangang was not cooperating due to a conflicting injunction issued by a Korean court. *Id.* at 626.

146. *See supra* note 98.

147. *See Globalsantafe*, 250 F. Supp. 2d at 623–24, for a summary of the court's reasons for finding that it could order a registry (VeriSign) to remove a domain name from a top-level domain zone file. The court indicated its willingness to enforce the statutory rights of trademark holders, even if such enforcement entailed asserting jurisdiction over a registry and overriding contracts within the ICANN hierarchy. "Simply put, the interest in vindicating congressionally provided trademark rights trumps contract." *Globalsantafe*, 250 F. Supp. 2d at 623. *See also infra* notes 158–59 and accompanying text, arguing that the differences between registrars and registries are largely artificial.

148. *See Globalsantafe*, 250 F. Supp. 2d at 622–23 (discussing, but not deciding, the question of whether the court could order a registry's unilateral deletion or transfer of a domain name); *see also* America Online, Inc. v. Aol.org, 259 F. Supp. 2d 449, 453–57 (E.D. Va. 2003). In *America Online Inc.*, the court extended the holding of *Globalsantafe* and actually ordered a registry to unilaterally transfer a domain name, reasoning that the only additional complexity arising from the order would involve coordination between the trademark owner/acquiring registrant and a registrar, which registrar could be chosen by the acquiring registrant. *Id.* at 455.

149. *See, e.g.*, Paul Schiff Berman, *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*, 153 U. PA. L. REV. 1819, 1823–34 (2005) (critiquing the *Globalsantafe* decision for being "founded solely on jurisdictional power and a race to the courthouse" and for not considering South Korean trademark law).

because it was confronted with a foreign litigant and a foreign court that was exercising jurisdiction over the case.[150]

In other cases with similar choice-of-law issues, the foreign domain name holder owned assets in the country where the lawsuit was filed. For example, in both the French *Yahoo!*[151] and the Australian *Dow Jones* defamation cases,[152] the foreign corporations, Yahoo! and Dow Jones, held assets in France and Australia, respectively, where the alleged harms occurred. The contacts created by these assets perhaps provided better justification for the French and Australian courts to assert jurisdiction because the foreign corporations could have avoided the reach of French and Australian law by not owning assets in those countries. In *Globalsantafe*, however, the foreign registrant's only asset within the United States was the domain name itself,[153] a fact which nonetheless provided enough justification for the court to assert jurisdiction. Like the foreign corporations in the *Yahoo!* and *Dow Jones* cases, the foreign registrant in *Globalsantafe* could have decided to avoid the reach of U.S. law by not owning any asset, including a domain name, in the United States.

At first glance, the results of *Globalsantafe* might seem to conflict with international-comity analyses and may also seem to be unfair to foreign registrants who want to take advantage of the popular .com, .org, and .net TLDs for their websites. However, the principles used in *Globalsantafe*—including a sovereign state's application of domestic law to an entity with an asset within its borders—are found in other conflicts-of-law and choice-of-law contexts, thus illustrating that the Internet context is unexceptional.[154] Furthermore, the popularity of a TLD should not provide a justification for relaxing jurisdiction.[155]

Additionally, in a subsequent case following *Globalsantafe*'s reasoning, the Eastern District of Virginia responded directly to the argument that an order requiring a U.S. registry to delete or transfer a domain name is unfair to foreign registrants. The district court replied that, when the registrants registered a .org

150. *See id.*

151. La Ligue Contre le Racisme et L'Antisemitisme (L.I.C.R.A.) and L'Union des Etudiants juifs de France (U.E.J.F.) v. Yahoo! Inc., Interim Court Order, The County Court of Paris 6, May 22, 2000. The original order and an English translation can be found in the Appendix to the Complaint for Declaratory Relief in Yahoo! Inc. v. L.I.C.R.A., 169 F. Supp. 2d 1181 (N.D. Cal. 2001), http://w2.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/20001221_yahoo_us_complaint.pdf (last visited June 7, 2007). For background on both the French Yahoo! case and the Australian Dow Jones case, see GOLDSMITH & WU, *supra* note 2, at 1–10, 147–61.

152. Dow Jones & Co. v. Gutnick, (2002) 210 C.L.R. 575 (Austl.), *available at* http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html.

153. That is, assuming one considers a domain name in a gTLD registry based in the United States as being a U.S. asset and assuming that one considers a domain name to be an asset or property—both of which are debatable but are not discussed here.

154. GOLDSMITH & WU, *supra* note 2, at 159–60 (referencing conflicts-of-law issues faced by multinational organizations in matters of healthcare, tax, consumer protection, and libel).

155. The popularity of the *.de* top-level domain does not require Germany to relax its jurisdictional law for British citizens, and vice versa for German citizens and the popular *.uk* top-level domain.

domain name with a U.S. registry, they "chose, in effect, to play Internet ball in American cyberspace."[156] The registrants must know or reasonably should know that under the ACPA a federal court in Virginia has jurisdiction over all .org domain names.[157] In addition, foreign registrants who wish to avoid the jurisdiction of U.S. courts may register their domain names in a ccTLD for which both the registry and the registrar are located outside the United States.

The reasoning in *Globalsantafe* also seems to extend the reach of a court's injunctive power under FRCP § 65(d). Even in the absence of a statute such as the ACPA, which specifically allows this *in rem* jurisdiction, a registry, as well as a registrar, should fall within FRCP § 65(d)'s "active concert or participation" analysis because the difference between registrars and registries are largely artificial.[158] One indication of this essentially artificial difference is the fact that NSI, the organization that preceded ICANN in administering domain names, performed both the duties of registrars and the duties of registries: NSI sold all the domain names in certain gTLDs, which later became the registrar function, and also administered the registry databases for those domains, which later became the registry function. It was only when governance functions were transferred to ICANN that ICANN and the DoC began to allow other entities to sell domain names as registrars in competition with NSI, with NSI continuing to act as the registry.[159] Although this event separated the registrar and registry function formally, these functions still could be performed by the same entity.

d. Injunctions Ordering Action by Regional Registries

Courts have also been willing to enjoin regional Internet registries.[160] In 2001, the Northern District of California issued an injunction ordering action by the American Registry of Internet Numbers (ARIN), the regional Internet registry for North America. The injunction was part of a long dispute over the domain name sex.com in the case of *Kremen v. Cohen*.[161] In 2006, Kremen brought a lawsuit to enforce the order and also alleged antitrust violations by ARIN. ARIN responded by challenging the court's power to issue the 2001 injunction under FRCP § 65(d) and requested, in the alternative, a clarification of the court's order. Although the court did not reach the merits of the antitrust allegations,[162] it did

---

156. Am. Online, Inc. v. Aol.org, 259 F. Supp. 2d 449, 457 (E.D. Va. 2003).

157. *Id.*

158. Harold Feld, *Structured to Fail: ICANN and the "Privatization" Experiment*, *in* WHO RULES THE NET? INTERNET GOVERNANCE AND JURISDICTION 333, 336 (Adam Thierer & Clyde W. Crews, Jr. eds., 2003).

159. *See* MUELLER, *supra* note 14, at 184–96.

160. *See supra* note 89 and accompanying text for a description of regional Internet registries.

161. Order RE: Registration of IP Numbers (Netblocks), In the Name of Judgment Creditors, Kremen v. Cohen, 5:06-cv-02554 (N.D. Cal. Sept. 17, 2001), *available at* http://eplaw.us/kremen/sept01order.pdf.

162. The court found that the statute of limitations had expired as to Kremen's antitrust allegations. Order Granting Defendant's Motion to Dismiss with Prejudice, Kremen v. American Registry For Internet Number, Ltd., No. C 06-2554 (N.D. Cal. Sept. 17, 2001), *available at* http://www.arin.net/media/dismissal-

clarify the order by directing the transfer of the IP numbers within ARIN's control.[163]

The case illustrates how far a court's injunctive power might extend up the DNS hierarchy, even to compel action by non-party regional Internet registries. Although regional Internet registries will not usually be involved in the enforcement of content, the case suggests that U.S. courts may order even high non-party actors in the DNS to transfer Internet resources. More generally, these cases demonstrate that nation-states will regulate regional Internet registries to the extent of their ability and that the geographic location of Internet resources is often determinative in which nation-state will regulate those resources.

e. *Injunctions Involving Country-Code Top-Level Domains*

As noted above, although almost all gTLDs have registries in the United States, ccTLDs do not. Regulating ccTLDs sites for content will require relying on the judicial systems of each individual country in which such registries are located, unless there is some other manner of establishing minimum contacts with the United States.

III. CONCLUSION

The contractual provisions imposed by ICANN, the administrator of the DNS, provide an avenue to enforce national laws regarding Internet content, most notably laws aimed at protecting children from Internet pornography. As head of the DNS, ICANN has substantial power over Internet actors, including registrars who sell domain names, registries who maintain databases of domain names, and regional Internet registries who allocate IP addresses. It has used this authority to implement not only technical policy, but also non-technical policy, largely at the encouragement of trademark interests.

ICANN has in place an elaborate structure of contracts and memorandums of understanding, as well as informal agreements, with many actors in the Internet hierarchy. These agreements contain the broad requirement that registrars must suspend, cancel, or transfer a domain name when ordered to do so by a court or when such action is required by ICANN in order to resolve disputes. This language in these ICANN-mandated contracts is sufficient to require suspension of a website upon receipt of a court order arising from the violation of an anti-pornography law.

An understanding of the contractual rights and duties among members of the DNS provides lawmakers and public interest groups with a framework around

---

granted.pdf.

163. Order Granting Motion for Clarification by Non-Party American Registry for Internet Numbers, Ltd., Kremen v. Cohen, No. C 98-20718 (N.D. Cal. Dec. 20, 2006), *available at* http://www.arin.net/media/clarification-granted.pdf.

which to craft enforcement mechanisms for laws regulating Internet content. Statutes providing for court orders to take down websites or forfeit domain names could be highly effective.

For such orders to be effective in the United States, a court must have jurisdiction over the parties and the ability to issue injunctions against non-party Internet actors. As we have seen, both of these requirements can be satisfied with regard to websites in nearly every gTLD. Domestic U.S. registrants are subject to *in personam* jurisdiction in the state and federal courts in the districts where they are domiciled and where they have minimum contacts. Foreign registrants registered with a domestic registrar are subject to jurisdiction in U.S. courts under ICANN's Registrar Accreditation Agreement, which requires that a registrar compel a domain name holder to submit to jurisdiction where the registrar is located. Foreign registrants of a domain name in a gTLD—including those registered with a foreign registrar—would fall within the jurisdiction of U.S. courts if Congress were to pass a statute with a jurisdictional scheme similar to the ACPA. Alternatively, U.S. courts may exercise jurisdiction over such registrants without new legislation through an *in rem* civil or criminal forfeiture action.

In addition, U.S. courts can issue injunctions against the primary entities involved in providing and regulating domain names on the Internet—registrars, registries, and regional Internet registries—under the "active concert or participation" language in FRCP § 65(d), with or even without legislation like the ACPA. Since the registries for ccTLDs are located outside the United States, however, these domain names would not be subject to jurisdiction in the United States.

Thus, the two major hurdles to the effective use of court orders in bringing down pornographic websites in most gTLDs—problems of jurisdiction and injunctive reach—are indeed surmountable. Opponents of pornography regulation in the United States frequently cite the inability to address pornography served offshore as the reason why it would be futile, or unconstitu-tional, to enact a statute regulating material harmful to minors.[164] But as this paper illustrates, tools for enforcing national pornography and obscenity laws already exist in ICANN's contractual structure. In addition, new technology such as geolocation filtering is removing some of the borderless nature of the Internet and rendering obsolete many of the rationales for limited jurisdiction over Internet actors. The failure of the United States to enact reasonable legislative regulation of the harmful pornography that has proliferated on the net is now inexcusable. If the United States is to retain its status as a leader in the development of civilization, especially in conceiving of ways to balance freedom and order, it must address

164. *See, e.g.*, ACLU v. Gonzales, 478 F. Supp. 2d 775, 810 (2007) (holding that the Children's Online Protection Act is underinclusive because "a significant amount of sexually explicit material on the Internet [] originates from outside of the United States" and the statute has no extraterritorial effect).

the new (but also archetypal and historical) conflicts of values that arise in the new world of cyberspace.

Finally, the United States did not just create the Internet, but also created its governing structure and charged ICANN with governing power. ICANN's hands are covered with non-technical policy choices, and it is now disingenuous to argue that ICANN cannot or should not help to mitigate the problem of Internet pornography. As ICANN has helped the big-roller money interests in protecting commercial values, such as trademarks, it can now certainly help save childhood for children.