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

Brent A. Little and Cheryl B. Preston[1]

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."[2] 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 a coordinated response extremely difficult. Individual countries are scrambling to find solutions. To combat pornography and other illegal online action, some countries 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.[3] 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. Even larger and more powerful countries have difficulty controlling illegal online conduct where offenders minimize their dependence on intermediaries,[4] thereby eliminating a government's means of

---

[1] Brent A. Little, J.D., 2007; Cheryl B. Preston, Edwin M. Thomas Professor of Law, Brigham Young University.
[2] RICHARD A. SPINELLO, CYBERETHICS: MORALITY AND LAW IN CYBERSPACE ix (3d ed. 2006).
[3] *See e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 81–84 (2006); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005).
[4] *See, e.g.,* Deborah Halbert, *Two Faces of Disintermediation: Corporate Control or Accidental Anarchy*, 2006 MICH. ST. L. REV. 83, 85\7–88 (2006) (citing examples of online actors circumventing government detection through the technology-facilitated elimination of intermediaries in areas of taxation, adoption, child pornography, and mail-order brides) (citations omitted).

regulating them. Offenders also evade prosecution by "mixing" legal and illegal conduct.[5] Some countries have even fewer methods in place to address abuses of cyberspace.

Of course, some countries, especially totalitarian countries, are approaching the problem of Internet pornography merely as 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, in this instance falling behind other countries in addressing the problem. All but the most limited regulatory efforts in the United States have been poorly conceived and out of touch with technology and, in any event, have failed to pass constitutional scrutiny.[6] In 1997, the United States Supreme Court struck down the Communications Decency Act (CDA), one of the United States Congress' first attempts to

[5] GOLDSMITH & WU, *supra* note 3, at 83–84 (stating that "mixing" occurs where illegal conduct (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 an unconstitutional state effort, see the Pennsylvania Solution discussed in Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003); Jim Hu, Court Strikes Down Pennsylvania Porn Law, CNET News.com, Sept. 10, 2004, http://news.com.com/Court+strikes+down+Pennsylvania+porn+law/2100-1028_3-5361999.html. The district court's 109-page memorandum opinion in the Pennsylvania case is available at http://www.cdt.org/speech/pennwebblock/20040910memorandum.pdf.

regulate online material that is "harmful to minors."[7] This is adult sexually explicit material that is not the very hard core pornography classified in the United States as "obscene"[8] or child pornography,[9] which is sexually explicit material using children in its production,[10] both of which are currently illegal. A year later, Congress responded by passing the Child Online Protection Act (COPA) to correct the constitutional defects in the CDA.[11] On a second trip, the Supreme Court again 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.[12] The case was then remanded back to the district court to determine whether filters do indeed offer sufficient protection for children against Internet pornography, and, if not, whether other grounds exist for finding COPA unconstitutional.[13]

On remand in *ACLU v. Gonzales*,[14] 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

---

[7] COPA defines "harmful to minors" as:

> any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that – (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

47 U.S.C. § 231 (e)(60).

[8] Obscenity is a limited category of hard-core pornography that is prohibited by law and without any First Amendment protection. The Supreme Court defines obscenity as material that:

> [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.

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

[9] *See* 18 U.S.C. 2251-2260.

[10] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

[11] Ashcroft v. American Civil Liberties Union, 542 U.S. 656 (2004).

[12] *Id*. at 666–69, 673.

[13] *Id.* at 672–73.

[14] American Civil Liberties Union v. Gonzales, 478 F.Supp.2d 775 (2007).

interest.[15] The court found that the statute is both overinclusive and underinclusive and that various affirmative defenses in the statute were not sufficient to make the statute narrowly tailored.[16] In addition, the court found that filters were a sufficiently effective, less restrictive alternative to COPA.[17] 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.

Because of intra- and inter-country regulatory difficulties, there is a need for more uniformity and international leadership in Internet regulation. The Internet Corporation for Assigned Names and Numbers (ICANN), the administrator of the domain name system (DNS), may provide some avenues to approach these problems. Although ICANN has resisted involvement in enforcement of Internet regulations, other entities in the Domain Name System (DNS) that ICANN supervises, known as registrars and registries—and the contractual obligations between those entities—may provide means of enforcing existing laws regulating online conduct.

This article first provides background on the history and structure of ICANN and then illustrates that, despite its claims to the contrary,[18] ICANN does do policy now in non-technical areas of Internet governance. This article then examines how ICANN structures and obligations within the Domain Name System (DNS) have been used to implement those policy objectives. Then we describe a piece of ICANN's extant policy structure that can be meaningfully engaged in helping countries carry out reasonable pornography regulation. This approach does not require radical changes in law or structure; instead, it enables governments to enforce existing

[15] *Id.* at 778–79.
[16] *Id.* at 834–837.
[17] *Id.* at 838–840.
[18] See *infra* notes 40–41 and accompanying text.

obscenity laws that are currently applicable in the Internet context but which 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 Internet service providers, provides the legal basis for removing Internet sites that violate the law. We then detail how this approach can be implemented in the United States under existing rules on jurisdiction and the reach of injunctions.

Our discussion takes place, of course, amid the overarching theoretical debate about whether, ultimately, a separate international legal regime or "cyberlaw" should be devised to coordinate the legal implications of a global internet or a pluralistic system arising from overlapping regulations adopted by each nation-state would be at least sufficiently workable, and keep power with individual nations.[19] At this time, Internet law, to the extent it exists, consists of nation-by-nation disparate rules and procedures, with the exception of ICANN policies, which are virtually universal because of its control over the Internet root system. We argue that ICANN can and does set policies and can take a more proactive stance with respect to pornography; and that its existing structure provides a virtually global enforcement mechanism. Moreover, this article demonstrates that, but because of the unique position of the United States with respect to primary Internet actors and its laws on jurisdiction, the nation-by-nation lay system permits a dominance of United States law.[20] Thus, a legal scheme that could be

[19] *See, e.g.*, H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. Marshall J. Computer & Info. L. 1, 4–8 (2005) (outlining the debate surrounding these two approaches, as led by Professors Johnson and Post (favoring a singular, global system), and Professor Goldsmith (favoring an overlapping pluralistic nation-by-nation approach)).
[20] *See infra* notes 120, 156, 163 and accompanying text.

formulated in the United States regulating material "harmful to minors,"[21] and the existing laws governing "obscenity"[22] and child pornography,[23] can be enforced by United States Courts with respect to much of the pornography posted outside of the United States.

I. ICANN CAN AND DOES NOW DO POLICY

Because ICANN was formed and enabled through a series of agreements involving the United States government and other Internet administrators, rather than by statute, its history follows complex and confusing turns.[24] A simple summary follows. Before ICANN's creation, domain name administration[25] was performed by Network Solutions Inc., a United States government contractor based in Virginia. In February 1998, the United States government initiated privatizing the management of domain names in a proposed regulation commonly known as the "Green Paper."[26] 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 domain name system.[27]

A short time later, the United States 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 that has been renewed various times over the years, first signed

[21] *See supra* note 7.
[22] *See supra* note 8.
[23] *See supra* note 9.
[24] For a detailed description of this process, see MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 141–208 (2002); *see also* 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).
[25] For descriptions of domain name fundamentals, see Mueller, *supra* note 24, at 30–56; Froomkin, *supra* note 24, 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).
[26] 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.
[27] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (Jun. 5, 1998), *available at*, http://www.icann.org/general/white-paper-05jun98.htm.

November 25, 1998.[28] Although the DoC declared that ICANN should assume certain functions under the White Paper, government contractors such as Network Solutions Inc. (NSI) continued to perform many of these functions without acknowledging ICANN's role. To correct this, in 1999, the 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.[29] ICANN and the United States government recently renewed their relationship in the form of a Joint Project Agreement (JPA) September 29, 2006.[30]

ICANN, a not-for-profit organization incorporated in California,[31] oversees the procedures by which domain names are assigned and given access to the root system over which electronic signals are sent on the World Wide Web.[32] It administers the Domain Name System (DNS), the system that resolves numerical Internet Protocol (IP) addresses from alpha-numeric domain names.[33] 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.[34] A domain name is the words, letters or symbols used to identify a webpage, such as CP80.org or ebay.com; the IP address is the unique set of numbers allocated to the computer on which that webpage is served so that messages will be properly routed to it. ICANN also administers the root or the root zone file which is one of the master control of all

[28] *See* ICANN's Major Agreements and Related Reports, ICANN, Oct. 31, 2006, http://icann.org/general/agreements.htm.
[29] *See generally* Froomkin, *supra* note 24, at 89–93.
[30] Joint Project Agreement, Sept. 29, 2006, http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/ICANNBoardResolution_09252006.htm.
[31] ICANN, Articles of Incorporation (As Revised Nov. 21, 1998), http://www.icann.org/general/articles.htm.
[32] *See* ICANN, ICANN Information, Mar. 26, 2007, http://icann.org/general/; ICANN, Bylaws, Section 1, Feb. 28, 2006, http://www.icann.org/general/bylaws.htm#II.
[33] For information about the DNS and its administration, see *supra* note 25.
[34] *See* Mueller, *supra* note 24, at 186–90, *188* (noting ICANN's "authority over almost all retain domain name registration"); A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, 2003 U. ILL. L. REV. 1, 18–20 (2003). *See also infra* notes 96–98 and accompanying text.

top-level domains (TLDs) – such as .com, .org., .asia – and their associated IP addresses.[35] Creating a new TLD involves adding the TLD to the root zone file.

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

Other aspects of ICANN's governance have not resulted in high-profile policies like the Uniform Domain Name Dispute Resolution Policy (UDRP), but still have significant influence on Internet management and regulation. For example, ICANN has authority over various entities in the Domain Name System (DNS) such as generic top-level domain (gTLD) registrars and registries.[36] ICANN 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 top-level domain (TLD). ICANN enters into contracts with these registrars and registries.[37] And through these contracts, ICANN is able to set technical standards for these entities.

But 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

[35] *See* Froomkin, *supra* note 24, at 17, 43–47, 89–90.
[36] ICANN also has agreements with sponsored top level domain (sTLD) and some country code top-level domain (ccTLD) registrars and registries, but many of these agreements are substantially different from the agreement with generic top-level domain entities and aren't analyzed here.
[37] ICANN does not have contracts with all registrars or registries around the world; for example, it does not have agreements with most registrars and registries of country-code top-level domains (ccTLDs). *See* ICANN, 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* Joint Project Agreement, Annex A: Affirmation of Responsibilities for ICANN's Private Sector Management, ¶ 5, Sept. 29, 2006, http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/ICANNBoardResolution_09252006.htm ("ICANN shall continue its efforts to achieve stable agreements with country code top-level domain (ccTLD) operators.").

holder is domiciled and where the registrar is located.[38] This provision has significant non-technical consequences.[39] In addition, because the provision is uniformly required across 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 Domain Name System (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."[40] The Department of Commerce originally called ICANN's function "coordination."[41] However, "technical decisions can have far-reaching economic and social consequences, altering the balance of power between competing businesses or nations and constraining the freedom of users. . . . The very passion with which stakeholders contest standards decisions should alert us to the deeper meaning beneath the nuts and bolts."[42]

Some commentators claim ICANN is a regulatory institution that wields quasi-governmental power and that engages in policymaking.[43] Some have stated that its mandate

[38] Registrar Accreditation Agreement, ICANN, § 3.7.7.10, 17 May 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm#3.
[39] *See infra* notes 99–101 and accompanying text.
[40] Dyson letter to Ralph Nadar and Jamie Love, June 15, 1999 (quoted in MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 8 (2002)).
[41] Management of Internet Domain Names and Addresses, 63 Fed. Reg. 31,741, 31,744 (1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm ("under the Green Paper proposal, the United States Government would gradually transfer these coordination function to the new corporation"); Froomkin, *supra* note 24, at 95.
[42] JANET ABBATE, INVENTING THE INTERNET 179 (3d ed., 2000).
[43] *See* Milton Mueller, *Why ICANN Can't*, IEEE SPECTRUM 15, 15 (July 2002); *see also* Froomkin, *supra* note 24, at 94–105; David Post, Governing Cyberspace, Jun. 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").

from the DoC to administer the Domain Name System (DNS) is similar to that of the United States Federal Communications Commission, which few would argue engages only in technical coordination.[44]

Perhaps initially, when administering the Domain Name System (DNS) was a one-person job with all the domain names and numbers recorded in a single notebook, administering the DNS was technical coordination. However, when domain name registration exploded under the oversight of Network Solutions, Inc. (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.[45]

ICANN took over various Internet governance functions previously performed by NSI in the late 1990s, and as the Internet has grown, ICANN's policy, gatekeeping, and business opportunity functions have increased. For example, ICANN caps the cost of registering a domain name.[46] It has taken a policy stand on the demand for domain names by controlling the number of new top-level domains.[47] Similarly, ICANN accredits a limited number of registrars, creating competition among prospective and existing registrars in what has become an extremely lucrative business.[48] 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.[49]

---

[44] *See, e.g.*, Mueller, *supra* note 43, at 16.
[45] MUELLER, *supra* note 24, at 120.
[46] *See* Mueller, *supra* note 43, at 16.
[47] *See* Mueller, *supra* note 43, at 16 ("ICANN . . . controls the supply of [domain] names by accepting or rejecting applications for top-level domains (.com, .net, and the like)").
[48] *See* ICANN, Accreditation Overview, Mar. 26, 2007, http://www.icann.org/registrars/accreditation.htm.
[49] *See* ICANN, Registry Services Evaluation Process, Mar. 26, 2007, http://www.icann.org/registries/rsep/.

ICANN prescribes many of the key contractual provisions that registrars must impose by contract on all applicants for domain names, and ICANN has also required modification of existing contracts to include the provisions.[50] It requires domain name holders to submit to an accelerated arbitration process to determine the scope of a party's trademark rights.[51] It determines the scope of domain name holders' personal privacy rights by setting policies for what personal information a registrar collects from domain name applicants upon registration under the WHOIS policy.[52] It sets technical standards for the administration of registration databases and the sharing of information among other Domain Name System (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."[53] 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.[54]

Perhaps the most influential interest group for whom ICANN has made policy is trademark holders and, more recently, United States copyright holders. "[T]he question of protection of trademarks [was] at the centre of the reform of Internet Governance, leading to the

[50] Froomkin, *supra* note 24, at 97.
[51] Mueller, *supra* note 43, at 16; Froomkin, *supra* note 24, 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"); Weinberg, *supra* note 47, at 216.
[52] ICANN, Whois Services, Mar. 26, 2007, http://icann.org/topics/whois-services/; ICANN, Public Participation Page, Whois Information Page, http://public.icann.org/whois#whatiswhois (last visited July 5, 2007) ("'Whois' refers to the information that is required whenever anyone registers a domain name").
[53] Mueller, *supra* note 43, at 16.
[54] 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.

establishment of ICANN in 1998."[55] Trademark holders were involved in the dialogue that shaped Internet governance almost from the beginning.[56] NSI created a trademark dispute resolution policy before ICANN was conceived.[57] 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 top-level domains. The trademark holders enlisted the United States Patent and Trademark Office and the Department of Commerce to help them argue that ignoring trademarks in relation to Internet governance would negatively impact commerce.[58]

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) due to trademark concerns.[59] These companies and others were also key players in bringing together a "dominant coalition" that negotiated what became known as the White Paper.[60]

The White Paper authorized the World Intellectual Property Organization (WIPO), "an entity entirely beholden to intellectual property owners,"[61] to propose a policy for handling trademark disputes. Since the time of the International Ad-Hoc Committee (IAHC) proposals, trademark interests had lobbied for a domain name management that was directly linked to trademark protection, centralizing the policing and enforcement of trademark holders' rights and shifting the transactions costs away from themselves.[62] The trademark interests attempted to implement this objective through WIPO, which initiated a consultation process to gather

---

[55] JOVAN KURBALIAJA & EDUARDO GELBSTEIN, INTERNET GOVERNANCE: ISSUES, ACTORS AND DIVIDES 80 (2005).
[56] *See* Mueller, *supra* note 43, at 73–208.
[57] *See supra* note 45 and accompanying text.
[58] MUELLER, *supra* note 24, at 137–39.
[59] *Id.* at 142–46, 154–60, 168–71.
[60] *Id.* at 168–75.
[61] *Id.* at 190.
[62] *Id.*

suggestions on trademark disputes.[63] WIPO's December 1998 interim report attempted to secure the strongest intellectual property protection imaginable.[64] It included, for example, a 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."[65] 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.[66]

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 wreck havoc on their registrant databases."[67] 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.[68] 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

---

[63] *Id.*
[64] *Id.* at 190–91.
[65] *Id.* at 190–91. 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.* at 191.
[66] *See id.* at 192–93.
[67] Judith Oppenheimer, Apr. 6, 2001, http://www.judithoppenheimer.com/pressetc/adentive.html (quoting a remark by Mr. Palage at a January 10, 2000 meeting of the Small Business Administration on domain name issues).
[68] MUELLER, *supra* note 24, at 193.

competition in registration by adding additional registrars.[69] Because it did not receive revenues as planned, ICANN had no financial support and went deeply into debt.[70] The benefactors who bailed ICANN out were, of course, the corporate interests who had the most stake in ICANN's survival. For instance, MCI loaned ICANN $500,000, and Cisco Systems loaned it $150,000.[71]

ICANN and its policies, especially the Uniform Domain Name Dispute Resolution Policy (UDRP), were the product of input by many interest groups, but particular influence was wielded by large corporations with huge economic stakes in protecting their trademarks and copyrighted material.[72] 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 intellectual property, and thus the financial interests, of big corporations 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.[73] In fact, interest groups representing the general public were clearly missing from the table when these initial policy decisions were made.[74] The general public at that time had little understanding of the Internet and 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.

---

[69] *Id.* at 194–95.
[70] *Id.* at 195.
[71] James Niccolai, *ICANN Survives on Corporate Dole*, THE INDUSTRY STANDARD, Aug. 20, 1999, http://thestandard.com/article/0,1902,6037,00.html.
[72] MUELLER, *supra* note 24, at 166–67, Table 8.1.
[73] *See e.g.*, *supra* note 65, listing parties who opposed WIPO's interim report.
[74] *See* KURBALIJA & GELBSTEIN, *supra* note 55, at 81 ("So far, copyright holders, represented by the major record and multimedia companies, have been more proactive in protecting their interests. The public interest has only been vaguely perceived and not sufficiently protected.").

Because ICANN has been the instrument for maintaining various public policies since its inception, there is no justification for its now arguing that it does not do "policy," and that it can't be socially responsible as well as economically driven. Given that reality, this paper suggests a possible avenue by which the obligations within ICANN's contracts can contribute meaningfully to the enforcement of obscenity 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 generic top-level domains (gTLDs). As governments become increasingly concerned about the 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 enforcement.

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

ICANN requires that all accredited registrars incorporate the Uniform Domain Name Dispute Resolution Policy (UDRP) by reference into all registration agreements with domain name holders.[75] The UDRP was established by ICANN and has been adopted by all accredited

[75] 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 . . . .

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

domain-name registrars of all generic top-level domains (gTLDs)[76] and a few country code top-level domains (ccTLDs).[77] 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. . . .[78]

The policy is incorporated by reference into the registration agreement between a registrar and a domain name holder.[79] 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 the contract.[80]

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

[76] ICANN, Domain Name Dispute Resolution Policies, 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).").
[77] ICANN, Uniform Domain Name Dispute Resolution Policy, Oct. 24, 1999 http://www.icann.org/dndr/udrp/policy.htm, Note 2 (explaining that the UDRP has been adopted by "all accredited domain-name registrars for domain names ending in .com, .net, and .org" and by "certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).").
[78] Uniform Domain Name Dispute Resolution Policy, ICANN, Oct. 24, 1999, http://www.icann.org/dndr/udrp/policy.htm.
[79] *Id.* ¶ 1 ("This Uniform Domain Name Dispute Resolution Policy . . . is incorporated by reference into your Registration Agreement. . . .").
[80] *Id.* n.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.")

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 governmentally authorized to adjudicate the claims brought before them.[81] Thus, if a court in the United States 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."[82]

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*.[83]

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."

---

[81] *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.").
[82] *Id.* ¶ 3. (emphasis added).
[83] Registrar Accreditation Agreement, ICANN, § 3.7.7.11, May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm#3 (emphasis added).

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.

Go Daddy, a large accredited registrar in the United States, for instance, uses a provision very similar to the above language in ICANN's accredited registrar agreement.[84] Another accredited registrar, 000Domain.com, uses even stronger language regarding power to cancel domain names.[85] 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*;[86] (c) *you use your domain in connection with unlawful activity*; or (d) you violate this Agreement.[87]

---

84 Go Daddy Domain Registration Agreement, Go Daddy Software, Inc., 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.

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

86 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).

87 *Id.* (emphasis added).

This language gives wide latitude to the registrar to unilaterally suspend or terminate a domain name. Subsection 16.3(c) would certainly cover the use of the domain to publish 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 contraction 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.[88]

With more aggressive language, another registrar, Tucows, reserves the right to suspend or cancel a domain name solely upon receiving notice of the filing of a complaint regarding the domain name.[89] 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.[90]

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

[88] *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.").
[89] *See* Tucows Reseller Contract, Tucows, http://resellers.tucows.com/contracts/tld/exhibita, (last visited Feb. 13, 2007).
[90] *Id.*(emphasis added).

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, recently the world's largest registrar, Go Daddy, suspended a website based on the website's content relying on authority from its terms of service, a separate agreement from its registration agreement, which allows Go Daddy to take down a site for any reason.[91] In that series of events, MySpace alleged that thousands of its users' passwords and 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.[92] Go Daddy indicated that it frequently removes domain

[91] See Declan McCullagh, GoDaddy pulls security site after MySpace complaints, CNET News.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, 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 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).

[92] Declan McCullagh, GoDaddy pulls security site after MySpace complaints, CNET News.com, Jan. 25, 2007, http://news.com.com/2100-1025_3-6153607.html?part=rss&tag=2547-1023_3-0-5&subj=news (quoting Go Daddy general counsel Christine Jones).

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."[93]

The contractual terms discussed in this section illustrate that (1) ICANN has strong bargaining power vis-á-vis registrars and registrants in the gTLDs, such that ICANN is able to mandate the use of specific contractual language between registrars and registrants; (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 Part B of this section, 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 between members of the Domain Name System (DNS) provides lawmakers and interest groups with a framework around which to craft legislation to regulate the Internet. First, 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 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 permits the disabling of means used to carry

[93] *Id.*

out illegal activity, already exist in various contexts that could be compared to regulation of pornography. For instance, under the Digital Millennium Copyright Act (DMCA), courts may impound any device or product related to the copyright violation, grant injunctions, or "order remedial modification or destruction of a violating device or product."[94] Similarly, the CANSPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing 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."[95] In countries without such legislation, 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.

1. Jurisdiction

In order for a court to hear a case, make a binding ruling, and then issue an order enjoining the continued availability of a web site, the court must have jurisdiction over the person or the thing—the person who controls the web site or the site itself. Generally, these will

[94] 17 U.S.C. § 1203.
[95] 18 U.S.C. § 1037.

be respectively a domain name holder and the domain name itself. The preferred basis for jurisdiction is *in personam*, and we address it first, followed by *in rem* jurisdiction.

Under United States law, the personal jurisdictional issues are slightly different for three classes of domain name holders: domestic registrants, foreign registrants registered with a United States-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.[96] Registries, on the other hand, are entities that administer a top-level domain (TLD).[97] A distinct type of registry is a Regional Internet Registry (RIR). Collectively, these entities are responsible for the allocation, registration, and administration of Internet Protocol (IP) numbers within a specific geographic location.[98] RIRs 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) we note is those domiciled in the United States. These domain name holders are subject to *in persona* jurisdiction in the state and federal courts in the districts where they are domiciled. They are also subject to jurisdiction in any other state or federal court where they have minimum contacts.[99]

b. Foreign registrants registered with a domestic registrar. The second category of domain name holders we note is foreign entities who register with a United States-based registrar. The ICANN Registrar Accreditation Agreement requires that a registrar compel a

[96] For a list of registrars accredited by ICANN, see ICANN, ICANN-Accredited Registrars, http://www.icann.org/registrars/accredited-list.html (last updated July 5, 2007).
[97] A list of registries is available at ICANN, Registry Listing, http://www.icann.org/registries/listing.html (last updated May 29, 2007).
[98] Early on it was decided that the management of domain names should be separate from the management of IP numbers. Daniel Karrenberg, Gerard Ross, Paul Wilson, & Leslie Nobile, Development of the Regional Internet Registry System, 4 THE 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.
[99] 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).

domain name holder to submit to jurisdiction both where the registered name holder is domiciled and where the registrar is located.[100] Any domain name holder, whether domiciled in the United States or not, who registers its domain name through a United States-based registrar, submits to jurisdiction where the registrar is located.[101]

c. Foreign registrants of a gTLD domain name registered with a foreign registrar. Third, we discuss domain name holders who are foreign registrants who register their domain names through foreign registrars. Normally, United States courts are unable to exercise jurisdiction over foreign brick-and-mortar entities because they do not have sufficient minimum contacts here.[102] However, as explained below, the minimum contacts test is not a serious hurdle for many and perhaps most pornographic websites operated by foreign registrants and registered with a domestic registrar.

The primary framework for considering minimum contacts created by a website was set forth in *Zippo Manufacturing Company v. Zippo Dot Com, Inc*., and has been adopted by perhaps all federal circuit appellate courts to consider the issue.[103] In *Zippo*, the court proceeded

---

[100] Registrar Accreditation Agreement, ICANN, § 3.7.7.10, 17 May 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.

[101] *Id.*

[102] See International Shoe Co. v. Washington, 326 U.S. 310 (1945), and its progeny.

[103] 952 F.Supp. 1119 (W.D.Pa. 1997). *See, e.g.*, Lakin v. Prudential Securities, Inc., 348 F.3d 704, 710 (8th Cir. 2003) (collecting cases from federal circuit courts addressing the issue of minimum contacts for specific jurisdiction arising from websites and noting that "[t]he great majority of these . . . have adopted the analytical framework of *Zippo*") (citing Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, (3d Cir.2003); ALS Scan, Inc. v. Digital Serv. Consult., Inc., 293 F.3d 707 (4th Cir.2002); Bensusan Rest. Corp. v. King, 126 F.3d 25 (2d Cir.1997); Cybersell, Inc., v. Cybersell, Inc., 130 F.3d 414 (9th Cir.1997); CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir.1996); Young v. New Haven Advocate, 315 F.3d 256 (4th Cir.2002)); Capitol Federal Sav. Bank v. Eastern Bank Corp., 2007 WL 1885134, *8 (D.Kan. 2007) ("The seminal authority for evaluating the extent to which Internet contacts may establish personal jurisdiction is *Zippo*").

As noted by the Eighth Circuit in *Lakin*, the majority of the federal courts of appeal cases it cited applied the *Zippo* test in asserting specific, but not general, personal jurisdiction over defendants. Lakin v. Prudential Securities, Inc., 348 F.3d 704, 710 (8th Cir. 2003). Obtaining specific jurisdiction over porn sites adequately facilitates the goals of this paper, which concerns jurisdiction and remedies relating to offenses stemming from the

from its basic conclusion, "consistent with well developed personal jurisdiction principles[,]" that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."[104] Recognizing the widely varying levels of commercial activity and interactivity websites offer to users, the court set forth a "sliding scale" analysis:

> At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.[105]

Pornographic websites exhibit the same continuum of commercial activity and interactivity described by the *Zippo* court. At one end are commercial porn sites that "clearly do[] business over the Internet"—and business is booming. One report indicates that revenue in the porn industry is increasingly coming from Internet sales (increasing by 14% in 2006), while, by contrast, revenues from DVD sales are dropping at an equal or greater rate (by up to 30% in

---

website content itself. *See* 18 Fletcher Cyc. Corp. § 8640.50 (2007) ("General jurisdiction arises when a nonresident defendant has continuous and systematic contacts with the forum state, while specific jurisdiction exists when the cause of action *arises out of or is related to the defendant's contacts with the forum*") (emphasis added).

For additional discussion of minimum contacts and *in personam* jurisdiction in relation to websites, see generally Richard E. Kaye, *Internet Web site activities of nonresident person or corporation as conferring personal jurisdiction under long–arm statutes and due process clause*, 81 A.L.R.5th 41 (2007).

[104] *Zippo*, 952 F.Supp. at 1124.

[105] *Id.* (citing, for each type of website mentioned, respectively, CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir.1996), Bensusan Restaurant Corp., v. King, 937 F.Supp. 295 (S.D.N.Y.1996), and Maritz, Inc. v. Cybergold, Inc., 947 F.Supp. 1328 (E.D.Mo.1996)).

2005 and 2006).[106] Under *Zippo* and its progeny, the greater number of sales contracts a website enters with users in the forum state, the more likely courts are to assert personal jurisdiction.[107]

At the other end of the continuum are passive porn sites that publish explicit material but do not significantly interact with end users and derive de minimis or no revenue from them. Here, courts are unlikely to assert *in personam* jurisdiction based on minimum contacts,[108] although other jurisdictional principles may apply.[109]

Middle-ground porn sites include those "where a user can exchange information with the host computer" and which require courts to "examin[e] the level of interactivity and commercial nature of the exchange of information that occurs on the Web site."[110] Courts will thus engage in a fact-intensive analysis of such interactive sites.[111] They are more likely to assert jurisdiction where the site manifests an intent to interact specifically with residents of a forum state[112] and

---

[106] Jon Swartz, *Purveyors of porn scramble to keep up with Internet*, USA TODAY, http://www.usatoday.com/tech/techinvestor/industry/2007-06-05-internet-porn_N.htm (last visited Aug. 2, 2007).

[107] *See, e.g.*, Bird v. Parsons, 289 F.3d 865, 874–75 (6th Cir.2002) ("We conclude that by maintaining a website on which Ohio residents can register domain names and by allegedly accepting the business of 4,666 Ohio residents, the Dotster defendants have satisfied the purposeful-availment requirement") (citing Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir.2002)).

[108] *See, e.g.*, American Girl, LLC v. Nameview, Inc., 381 F.Supp.2d 876 (E.D.Wis. 2005) (declining to assert personal jurisdiction based on "passive" porn site: "Doe's web site does little more than make information available. Doe does not sell goods or services nor solicit business through the site. Indeed, there is no evidence that Doe ever made any contact with anyone in Wisconsin through the web site. Thus, the web site is passive.").

[109] A court will, for example, weigh contacts created by a website along with *non*-cyber contacts between the domain name holder and the forum state in its minimum contacts analysis. *See* Richard E. Kaye, *Internet Web site activities of nonresident person or corporation as conferring personal jurisdiction under long–arm statutes and due process clause*, 81 A.L.R.5th 41, §§ 4, 4.5, 7 (2007) (collecting cases).

For additional approaches to *in personam* jurisdiction, see *infra* notes 114–115 and accompanying text; see *infra* Parts II.B.1.c.(1) and (2) for *in rem* jurisdiction theories.

[110] *Zippo*, 952 F.Supp. at 1124.

[111] *See* Richard E. Kaye, *Internet Web site activities of nonresident person or corporation as conferring personal jurisdiction under long–arm statutes and due process clause*, 81 A.L.R.5th 41, §§ 6[a], 6[b] (2007) (collecting cases).

[112] Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 ("A defendant purposefully avails itself of the privilege of acting in a state through its website if the website is interactive to a degree that reveals specifically intended interaction with residents of the state") (citing *Zippo*, 952 F.Supp. at 1124); Dedvukaj v. Maloney 447 F.Supp.2d 813, 820–22 (E.D.Mich. 2006); *cf.* Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 454–55 (3d. Cir. 2003) (finding that website operated by Spanish corporation, with exclusively Spanish-language content; customer input features incapable of accommodating United States addresses; and only two sales to persons in the United States indicated that, without further evidence, website was insufficient basis to assert specific jurisdiction). *See also* Goldhaber v. Kohlenberg, --- A.2d ----, 2007 WL 2198181, *1–*5 (N.J.Super.A.D. 2007) (affirming

where the website manifests high levels of interaction or commercial activity with residents of the forum state.[113]

Thus, through their websites, many foreign registrants registering a name in a generic top-level domain (gTLD) with a United States-based registry are purposefully availing themselves of the laws and protections of a United States jurisdiction, satisfying the "purposeful availment" test.[114] Moreover, even this "purposeful availment" may not be required. Many commentators suggest that personal jurisdiction may be based solely on effects in the United States without any requirement of "purposeful availment."[115]

---

exercise of jurisdiction over nonresident defendant in a defamation suit based on statements posted by defendant online. Exercise of jurisdiction was appropriate because defendant's allegedly defamatory online postings referenced particular individuals, a police department, and a municipality within the forum state, showing that defendant knowingly targeted the forum state and thus should have reasonably anticipated being haled into court there).

[113] *See, e.g.*, *Neogen*, 282 F.3d 883, 890–91 (6th Cir. 2002) (finding that issuing passwords to residents of Michigan "as part of a contract" for website services and "hold[ing] itself out as welcoming Michigan business" were factors "support[ing] a finding of purposeful availment[,]" although court did not decide the issue); First Tennessee Nat. Corp. v. Horizon Nat. Bank, 225 F.Supp.2d 816, 821 (W.D.Tenn.2002) (asserting specific jurisdiction over website operator because it "permit[ted] Tennessee residents to obtain mortgage loans, obtain expert loan advise, and receive daily commentary"); *cf.* Carefirst Of Maryland, Inc. v. Carefirst Pregnancy Centers, Inc., 334 F.3d 390, 394–95, 398–401 (4th Cir. 2003) (describing "semi-interactive" website that "solicit[ed] donations; educate[d] pregnant women about nutrition, infant care, and prenatal care; provide[d] references to Chicago-area medical doctors and hospitals; promote[d]s its counseling services and parenting classes; and advertise[d] the pregnancy tests and ultrasound services that it offers free of charge[,]" and had received apparently $1524 in donations from residents of forum state (not through the website, except for one online donation made by plaintiff's counsel), had "strongly local character" insufficient for forum state to assert jurisdiction).

[114] *See also* Lee, *supra* note 125, 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, http://www.caslon.com.au/securityguide14.htm (last updated July 2005). Similarly, geolocation filtering permits an online publisher to vary or restrict the content of her website based on users' geographical location. *See* Wayne Madsen, Internet Censorship: The Warning Signs Were Not Hidden, Dec. 9, 2005, *available at* http://www.prisonplanet.com/articles/december2005/091205nothidden.htm (last visited July 6, 2007). 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.

[115] *See* 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, 604 (2006) (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 114, at 1955 & n.25 (listing cases that

Aside from the personal jurisdiction framework set forth in case law, United States courts may also exercise jurisdiction over foreign registrants of a domain name in a generic top-level domain (gTLD) by passing a statute with a jurisdictional scheme similar to the Anticybersquatting Consumer Protection Act (ACPA). Alternatively, United States 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 ACPA. Some United States statutes provide means for obtaining jurisdiction over foreign domain name holders. The Anticybersquatting Consumer Protection Act (ACPA) provides trademark holders with civil remedies against defendants who obtain domain names in "bad faith."[116] 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.

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

---

"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 using an effects jurisdictional analysis in other areas of law such as securities as well. Consolidated 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 tender offer of securities by foreign entities had "sufficient effects within the United States" to permit 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. Dow Jones & Co. v. Gutnick (2002) 210 C.L.R. 575 [Austl.], available at http://www.4law.co.il/582.htm (Australia); Richardson v. Schwarzenegger, 2004 EWHC 2422 (Q.B. Oct. 29, 2004), available at http://portal.nasstar.com/75/files/Richardson-v-Schwarzenegger%20QBD%C2029%C20Oct%2004.pdf (England).

[116] 15 U.S.C. § 1125(d)(1)(A)(i) (2006). "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 Services, Ltd. v. Epix, Inc., 304 F.3d 936, 946 (9th Cir. 2002) (citing Virtual Works, Inc. v. Volkswagen of America Inc., 238 F.3d 264, 267 (4th Cir.2001)).

the domain name is located" under certain conditions.[117] Although the trademark holders cannot reach the third category—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.[118] In practice, this provision permits a United States court to obtain jurisdiction over an infringing website when foreign domain name holders using foreign registrars are unavailable by service of process. Since almost all unsponsored[119] generic top-level domains (gTLDs) have their headquarters or an office in the United States, nearly all registrants of gTLD domain names are subject to the ACPA.[120] Passing legislation with an approach similar to the ACPA that addresses online pornography would simplify many jurisdiction problems.

[117] *Id.* § 1125(d)(2)(A).
[118] *Id.*
[119] 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 (gTLDs), Mar. 26, 2007, http://www.icann.org/tlds/.
[120] 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, May 29, 2007, http://www.icann.org/registries/listing.html; 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).

(2) *In rem* jurisdiction in a forfeiture action. Although the ACPA is a trademark statute, it may be adapted to fit the pornography context. But the pornography problem may even more appropriately fit into existing common law *in rem* jurisdiction.[121]

For instance, under federal obscenity[122] 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.[123] Such a seizure action requires a warrant based on a probable cause, showing the property's involvement (usually as a tool or instrumentality in the commission of a crime involving obscenity), and requires a finding that the material is obscene under federal law.[124]

Such an *in rem* civil forfeiture action requires that the property have a situs within the United States.[125] Under the ACPA, courts have determined that Congress intended that a domain name be treated as property and that its situs is in the location of the registrar or registry that registered or assigned the domain name.[126] In a federal obscenity case, where there would be no

---

[121] *See* Porsche Cars N. Am., Inc. v. Porsche.net, 302 F.3d 248, 260–262 (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).

[122] Obscenity is a limited category of hard-core pornography that is prohibited by law and without any First Amendment protection. The Supreme Court defines obscenity as material that:

> [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.

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

[123] 18 U.S.C. § 1467(a), (c). 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 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); 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).

[124] 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").

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

[126] 15 U.S.C. § 1125(d)(2)(A) (2006); Porsche Cars North America, Inc. v. Porsche.Net, 302 F.3d 248 (4th Cir. 2002) (upholding the constitutionality of the ACPA's *in rem* jurisdictional provisions). *But see* Catherine T. Struve

statutory statement of situs such as in ACPA, the common law could reach a similar conclusion since the registrar or registry are the entities who control domain names.[127]

Thus, courts may assert *in rem* jurisdiction 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. This conclusion follows from the continuing viability of the territoriality framework in *Pennoyer v. Neff*[128] recently reaffirmed in *Burnham v. Superior Court*.[129] In *Burham*, the 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.'"[130] However, United States Supreme Court jurisprudence may require that, in the context of *in rem* proceedings, a party must still satisfy the minimum contacts analysis applicable in *in personam* proceedings, as discussed above.[131]

This section illustrates that using the existing common law or a statute following the jurisdictional framework of the ACPA would permit either an aggrieved party or the government to bring an *in rem* action against a domain name, whether held by a foreign or domestic holder, as long as the foreign domain name holder uses either a domestic registrar or (almost) any generic top-level domain. The reach of this jurisdiction extends to all websites using .biz, .com,

---

and R. Polk Wagner, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 17 BERKELEY TECH. L.J. 989 (2002).

[127] *See* Lee, *supra* note 125, at 126–37 (arguing that domain names have their situs where the entity, the registrar or registry, controlling the property is located).

[128] 95 U.S. 714 (1877).

[129] 495 U.S. 604 (1990).

[130] *Id.* at 619; 4 Charles Alan Wright & Arthur Miller, Federal Practice and Procedure 1073 (2d ed. 1987 & Supp. 1999); Lee, *supra* note 125, at 137–141.

[131] *See* Shaffer v. Heitner, 433 U.S. 186, 212 (1977) ("[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 also* Lee, *supra* note 125, at 139. The minimum contacts analysis applicable to websites is discussed in *supra* notes 103–114 and accompanying text.

.info, .int, .name, .net, .org, or .pro.[132] But, these approaches would not permit jurisdiction in the United States to two important country code top-level domains, .uk and .de, which are two of the five largest top-level domains,[133] and these domain holders would not be subject to suit in the United States unless they used a United States 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 still must issue an order that will be effective to reach a registrar or registrant with the contractual obligations discussed above in Part II.A. A United States 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 (RIRs), and entities involved with country-code top-level domains.

a. General injunctive reach. Section 65(d) of the FRCP provides that an order granting an injunction "is binding only upon the parties to the action, their officers, agents, servants, employees, and attorneys, and upon those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise."[134] Thus, the general

---

[132] *See* supra note 120.
[133] VeriSign, *The VeriSign Domain Report*, 3 THE 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.").
[134] Fed. R. Civ. Proc. 65(d); *see* Ronald I. Mirvis, 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).

rule is that nonparties are not usually bound by injunctions. However, 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."[135] This "active concert or participation" language has been interpreted to include "situations where a nonparty with actual notice aids or abets a named defendant or his privy in violating the order."[136] 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.[137]

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.[138] In a case brought in the United States District Court for the Eastern District of Pennsylvania, *Worldsport Networks Ltd. v. ArtInternet S.A.*, a French company admitted to infringing an Irish corporation's trademark on the domain name "worldsport.com."[139] The court noted that, since the parties stipulated that the plaintiff's

[135] 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); 61 A.L.R. FED. 482 § 6[a] (collecting cases).
[136] *Reliance*, 84 F.3d at 377.
[137] *Id.*
[138] Worldsport Networks Ltd. v. Artinternet, S.A., No. CIV. A. 99-CV-0616, 1999 WL 269719, (E.D. Pa. Apr. 28, 1999 at *1).
[139] *See id.*

trademark rights were violated, the defendants should be enjoined from future violation.[140] 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."[141] 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."[142]

Critics of this expanded view may argue that this reasoning may be dicta because NSI did not object to the injunction and had a policy that required it to obey a court's final order without being made a party to the litigation.[143] NSI had, in fact, reminded the plaintiff of that policy.[144] 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 defendant, the court noted that "NSI has consented to this exercise of the Court's authority."[145]

Whether the court's FRCP § 65(d) analysis is dicta or not, both readings of the case are helpful precedent 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.[146] Thus, even if the court's ruling is dicta, the existing contracts provide the same alternate basis for relief as that relied upon in *Worldsport*. If

[140] *See id.* at *3.
[141] *Id.*
[142] *Id.*
[143] *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").
[144] *See id.* at *1–*2.
[145] *Id.*
[146] *See supra* Part II.A.

the reasoning is not dicta, then the case is strong authority for the proposition that registrars are in active concert or participation with their own domain name registrants.

Requiring "innocent" registrars to suspend domain names for offending web content with injunctions 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, 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."[147] An injunction requiring a registrar to suspend a domain name that hosts obscene content under federal 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.[148] If the United States were to adopt a measure proscribing the publishing of material harmful to minors[149]—including pornography that does not satisfy the *Miller* obscenity test,[150] as well as obscenity and child pornography—jurisdiction and the mechanisms for enforcement of injunctions to remove such content, even if published overseas, are already largely available.

In addition, 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

[147] *See* Coca-Cola Co. v. Gemini Rising, Inc., 346 F.Supp. 1183, 1193 (E.D.N.Y. 1972); 15 U.S.C. § 1114(2)(A); Worldsport Networks Ltd. v. ArtInternet S.A., 1999 WL 269719, (E.D. Pa. Apr. 28, 1999 at *3).
[148] 18 U.S.C. § 1467(a), (c).
[149] For an example of proposed regulation, see Cheryl B. Preston, Scott R. Rasmussen, & Allan Smart, *Children and Internet Pornography: The Nature of the Problem and the Technologies for a Solution* (prior article).
[150] *See, supra,* note 122.

nonparties. Section 230 of the Communications Decency Act,[151] upheld by the Supreme Court, contains a provision that addresses a similar issue.[152] Section 230 protects a "provider or user" of an "interactive computer service"[153]—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.[154] So a registrar that suspends a domain name in good faith to restrict access to the objectionable material as directed by court order is not liable to the domain name holder based on this provision. 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.

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 Anticybersquatting Consumer Protection Act (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."[155] Legislation that enforces pornography standards and that parallels the ACPA would allow the suspension of offending domain names through court orders directed at registries (the entities in charge of top level domains (TLDs)), not just 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

[151] 47 U.S.C. § 230.
[152] Reno v. American Civil Liberties Union, 521 U.S. 844, 861–64 (1997) (holding unconstitutional §§ 223(a)(1) and 223(d) of the CDA under the First Amendment because they are overbroad, but not other provisions of the Act including § 230).
[153] 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).
[154] 47 U.S.C. § 230(c); Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).
[155] 15 U.S.C. § 1125(d)(2)(A).

United States court's injunction if using a generic top-level domain headquartered in the United States.[156]

A number of courts have upheld this application of the ACPA to registries and not just to registrars. For example, 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 in *Globalsantafe Corporation v. Globalsantafe.com*.[157] In *Globalsantafe* a trademark owner brought an infringement action against an alleged cybersquatter located in Korea under the ACPA.[158] 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.[159]

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.[160] The court appeared cautious in extending its reach beyond the Korean registrar to a higher level in the Domain Name System (DNS), the United States-based registry VeriSign, even though the ACPA's language refers to both the registrar and the registry.[161] 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 top-level domain (TLD) names administered by VeriSign meant that this court

[156] *See supra* note 120.
[157] 250 F. Supp.2d 610, 617 (E.D. Va. 2003).
[158] *Id.* at 612–13.
[159] *Id.* at 613–14.
[160] *Id.* at 617–24.
[161] *See e.g.*, 15 U.S.C. § 1125(d)(2)(A) (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").

would likely be asked to assert jurisdiction over domain names owned all over the world.[162] Nonetheless, the court asserted jurisdiction.

The *Globalsantafe* opinion is significant, first, because it shows that a court will extend its jurisdictional and enforcement reach up the Domain Name System (DNS) hierarchy to registries even when doing so subjects a large number of domain names held by foreign registrants through foreign registries to jurisdiction in United States courts. This decision subjects nearly all registrants of generic top-level domains (gTLDs) to jurisdiction in the United States even though they might only contract with a foreign registrar because the registries of nearly all gTLDs are located in the United States.[163]

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.[164] Third, the decision shows that a United States court may require

---

[162] *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 country code top-level domains (ccTLDs), which would impede enforcement of United States trademark rights 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 TLD 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 . . . interfere with the 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.

[163] *See supra* note 120.

[164] See *supra* note 162 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 175–176 and accompanying text, which illustrate that the differences between registrars and registries are largely artificial.

registries located in the United States to unilaterally delete and even unilaterally transfer[165] domain name registrations even 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.[166] The *Globalsantafe* court only engaged in an international-comity analysis instead of a full choice-of-law analysis when confronted with a foreign litigant and a foreign court also exercising jurisdiction over the case.[167] 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![168] and the Australian Dow Jones defamation cases,[169] the foreign corporations, Yahoo! and Dow Jones, held assets in France and Australia, respectively, where the alleged harms occurred. The existence of assets created contacts that perhaps better justified the exercise of jurisdiction by the French and Australian courts because the foreign corporation could have decided to avoid the reach of French and Australian law by not owning assets in those countries.

---

[165] *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.

[166] *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).

[167] *See id.*

[168] 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. and Yahoo France, 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. and U.E.J.F., 169 F.Supp. 2d 1181 (N.D. Cal. 2001), http://www.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 3, at 1–10, 147–61.

[169] Dow Jones v. Gutnick, [2002] HCA 56, 2002 AUST HIGHCT LEXIS 61 (High Court of Australia).

In *Globalsantafe*, however, the foreign registrant's only asset within the United States was the domain name itself.[170] But this fact was enough for the court.

Although the result in *Globalsantafe* seems to contrast with the factual scenarios in the French Yahoo! and Australian Dow Jones cases, the rationales of the three cases may be reconciled. The foreign registrant in *Globalsantafe* could have avoided the jurisdictional reach of United States courts by not registering its name in a top-level domain (TLD) whose registry is located in the United States. Like the foreign corporations in the Yahoo! and Dow Jones cases, the foreign registrant in *Globalsantafe* could have decided to avoid the reach of United States law by not owning any asset, including a domain name, in the United States

At first glance, the results in *Globalsantafe* might seem to conflict with an international-comity analysis and to be unfair to foreign registrants who want to take advantage of the popular .com, .org, and .net top-level domains (TLDs) for their websites. Upon closer examination, however, it becomes clear that 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, illustrating that the Internet context is unexceptional.[171] Second, the popularity of a TLD should not be an argument for relaxing jurisdiction.[172]

Third, in a subsequent case following *Globalsantafe*'s reasoning, the Eastern District of Virginia directly responded to the argument that an order requiring a United States registry to delete or transfer a domain name is unfair to foreign registrants. The district court in Virginia

[170] That is, assuming one considers a domain name in a gTLD registry based in the United States as being a United States 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.
[171] GOLDSMITH & WU, *supra* note 3, at 159–60 (referencing conflicts-of-law issues faced by multinational organizations in matters of healthcare, tax, consumer protection, and libel).
[172] 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.

replied that, when the registrants registered a .org domain name in a United States registry, they "chose, in effect, to play Internet ball in American cyberspace."[173] The registrants must know or reasonably should know that under the ACPA a federal court in Virginia has jurisdiction over all .org domain names.[174] In addition, foreign registrants who wish to avoid United States courts may register their domain names in a country code top-level domain (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.[175] One indicator that the difference is essentially artificial 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 previously sold all the domain names in certain generic top-level domains (gTLDs), which later became the registrar function, and also administered the registry databases for those gTLDs, 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 for those gTLDs.[176] This event separated the registrar and registry function formally, although those functions could still have been performed by the same entity.

---

[173] *America Online, Inc.*, 259 F.Supp.2d at 457.
[174] *See id.*
[175] 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).
[176] *See* MUELLER, *supra* note 24, at 184–96.

d. Injunctions ordering action by regional registries. Courts have also been willing to enjoin Regional Internet Registries (RIRs).[177] 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 *Kremen v. Cohen*.[178] In 2006, Kremen brought a lawsuit to enforce the order and also alleged antitrust violations by ARIN. ARIN responded by challenging the issuing court's injunctive power under FRCP § 65(d) to issue the 2001 injunction and in the alternative requesting clarification of the court's order. Although the court did not reach the merits of the antitrust allegations,[179] it did clarify the order by directing the transfer of those IP number blocks within ARIN's control.[180]

The case illustrates how far a court's injunctive power might extend up the Domain Name System (DNS) hierarchy even to compel action by a non-party regional Internet registry (RIR). Although RIRs will not usually be involved in the enforcement of content, the case suggests that courts may order even high Domain Name System (DNS) non-party actors to transfer Internet resources. This result further suggests that courts will not be dissuaded from enjoining Domain Name System (DNS) bodies that administer resources that many believe should not be subject to any one sovereign and whose actions have implications for foreign individuals and countries and the Internet globally. More generally, these cases demonstrate that nation-states will regulate RIRs 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.

---

[177] See *supra* note 98 and accompanying text for a description of RIRs.
[178] Order RE: Registration of IP Numbers (Netblocks), Kremen v. Cohen, 5:06-cv-02554, Sept. 17, 2001, *available at* http://eplaw.us/kremen/sept01order.pdf.
[179] The court found that the statute of limitations had expired as to Kremen's antitrust allegations. Kremen v. American Registry For Internet Number, Ltd., No. C 06-2554, Order Granting Defendant's Motion to Dismiss with Prejudice, Dec. 20, 2006, *available at* http://www.arin.net/media/dismissal-granted.pdf.
[180] Kremen v. Cohen, No. C 98-20718, Order Granting Motion for Clarification by Non-Party American Registry for Internet Numbers, Ltd., Dec. 20, 2006, *available at* http://www.arin.net/media/clarification-granted.pdf.

e. Injunctions involving country code top-level domains. As noted above, although almost all generic top-level domains (gTLDs) have registries in the United States, country code top-level domains (ccTLDs) do not. Regulating ccTLD sites for content will require relying on the judicial systems of each individual country in which such domains are located, unless there is some other manner of establishing minimum contacts with the United States. It might be possible to sue in the United States based on the effects the website has in the United States, but the plaintiff would need to establish some situs where the domain name is located for the *in rem* action. Since the registries are likely located in the applicable country, these domain names would not be subject to jurisdiction in the United States.

CONCLUSION

ICANN, the administrator of the domain name system (DNS), may provide some avenues to control illegal online content and to protect 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.[181]

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. In particular, ICANN's contracts with registrars of generic top-level domains (gTLDs) can be meaningfully engaged in helping countries carry out reasonable pornography regulation. These agreements broadly require registrars to suspend, cancel, or transfer a domain name when ordered by a court[182] or required by ICANN for resolution of disputes.[183] This language, existing

[181] *See supra* Part I.
[182] *See supra* notes 75–82 and accompanying text.

in ICANN-mandated contracts, is sufficient to require suspension of a website upon receipt of a court order arising from anti-pornography laws. Using this current structure, both ICANN and accredited registrars could set standards and enforcement procedures by contract with domain name owners who publish pornography.

Understanding the contractual rights and duties between members of the Domain Name System (DNS) provides lawmakers and interest groups with a framework around which to craft legislation to regulate the Internet. Interested parties should maximize the use of existing legislation that allows a private party or public official to obtain a court order requiring illegal material to be taken off the web.

For such an order to be effective, 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 on most generic top-level domains.[184] Domestic registrants are subject to *in persona* 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 United States 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 generic top-level domain (gTLD)—even those registered with a foreign registrar—would fall within the jurisdiction of United States courts if the United States were to pass a statute with a jurisdictional scheme similar to the Anticybersquatting Consumer Protection Act (ACPA). Alternatively, United States courts may exercise jurisdiction over such registrants without new legislation through an *in rem* civil forfeiture action.

---

[183] *See supra* note 83 and accompanying text.
[184] *Supra* Part II.B.

Similarly, federal courts can issue injunctions against the primary entities involved in providing and regulating domain names on the Internet—registrars, registries, and regional Internet registries (RIRs)—under the "active concert or participation" language in FRCP § 65(d), with or even without legislation like the ACPA. Since the registries for ccTLD sites 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 on most generic top-level domains—problems of jurisdiction and injunctive reach—are indeed surmountable. The architecture is already in place and recognized by contract in all of ICANN's dealings, as well as the existing contracts of registrars and domain name holders. Reformers in various countries should follow the lead of the United States and other countries[185] by urging their own legislative bodies to set standards and pass laws giving courts jurisdiction to order the termination of domain names and the taking down of sites used to publish illegal pornography. In the United States, statutes following this model already exist in various contexts that could be compared to regulation of pornography. As noted above, the Digital Millennium Copyright Act (DMCA) authorizes courts to order the impounding of any device or product involved in a copyright violation, grant injunctions, or "order remedial modification or destruction of a violating device or product."[186] Similarly, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM 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."[187] The Anti-Cybersquatting Act (ACPA), also discussed above, has the most direct language on this kind of enforcement,

[185] *See e.g.*, GOLDSMITH & WU, *supra* note 3, at 73; Perdue, *supra* note 115, at 470 & n.99.
[186] 17 U.S.C. § 1203.
[187] 18 U.S.C. § 1037.

providing for "forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark."[188]

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 to create a United States statute.[189] But as this paper illustrates, the failure of the United States to enact reasonable legislative regulation of the harmful pornography that has proliferated on the net is inexcusable and an embarrassment to the country that introduced the Internet, its evils as well as its blessings, to the world. The free world has modeled governments after the United States Constitution and the wealth of American legal structures and content. If we are to retain our status as a leader in the development of civilization, especially in conceiving of ways to balance freedom and order, we must address the new (but also archetypal and historical) conflicts of values that arise in the new world of cyberspace.

And, finally, the United States, like Dr. Frankenstein, created not just the Internet, but also its governing structure and gave power over it to ICANN. ICANN's hands are covered with non-technical policy choices; it is disingenuous to now argue ICANN "can't" help with the problem of Internet pornography. ICANN helped the big-roller money interests in protecting commercial values, such as trademarks. It can now help save childhood for children.

[188] 15 U.S.C. § 1125(d)(2)(D).
[189] *See, e.g.*, American Civil Liberties Union v. Gonzales, 478 F.Supp.2d 775 (2007).