Washington and Lee Law Review

Volume 74 | Issue 3 Article 3

Summer 6-1-2017

Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation

Annemarie Bridy
University of Idaho College of Law

Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation

Annemarie Bridy*

Table of Contents

* Professor of Law, University of Idaho College of Law; Affiliate Scholar, Stanford Center for Internet and Society (CIS); Affiliated Fellow, Yale Law School Information Society Project. Versions of this Article were presented at "Intellectual Property in All the New Places" at Texas A&M Law School, IPSC 2016, PLI's 2016 Intermediary Businesses Roundtable, and "Speech, Law, and Borders" at Stanford CIS. The author would like to thank Neil Brown, Michael Froomkin, Kathy Kleiman, David G. Post, Mitch Stoltz, and Rebecca Tushnet for helpful feedback during the drafting process.

I. Introduction

Enforcing intellectual property rights through the administration of the Domain Name System (DNS)—the Internet's addressing system—is not a revolutionary development. Trademark rights have been enforced to a limited extent within the DNS since 1999, when the Internet Corporation for Assigned Names and Numbers (ICANN)—the specially-created entity that oversees governance and administration of the DNS—introduced the Uniform Domain Name Dispute Resolution Policy (UDRP) for adjudicating fights over domain names containing trademarked words and phrases.[1]

Copyright enforcement, by contrast, has never been ICANN's bailiwick; nor has it been the province of DNS registries or registrars—the intermediaries that operate the DNS on a day-to-day basis under contract with ICANN.[2] ICANN has historically recognized that its role as an online intellectual property enforcer stops at trademarks in domain names and does

1. *See Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy*, ICANN, https://www.icann.org/resources/pages/schedule-2012-02-25-en (last visited Sept. 20, 2017) [hereinafter *Timeline*] (providing links to historical documents relating to the formulation, approval, and implementation of the UDRP) (on file with the Washington and Lee Law Review).

2. These intermediaries include ICANN-approved registry operators (or registries) and registrars. For each Top Level Domain (TLD), there is one registry operator responsible for the master database of all domain names in that "zone" and for the operation of that TLD's authoritative name servers, which look up location information in response to user queries. *See* NAT'L RESEARCH COUNCIL, SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION 125–26 (2005) [hereinafter SIGNPOSTS] ("ICANN has been delegated authority by the [Department of Commerce (DOC)] (and subject to DOC's approval) over entries in the root zone and, consequently, it can determine which organization is delegated responsibility for each ccTLD and gTLD."). Registries contract with various registrars to sell and register domain names to members of the public. *See id.* at 136–38 (explaining the relationship between registries, registrars, and registrants).

not extend to copyrights in online content.[3] Its public messaging on this point is quite clear.[4]

In recent years, however, ICANN has faced increasing pressure from corporate copyright holders, who believe that all online intermediaries, including those that operate the DNS, should be responsible for enforcing copyrights.[5] Although ICANN has continued to resist direct involvement in copyright enforcement activities, it accommodated right holders in 2013 by altering its contracts with DNS intermediaries to support a system of extra-judicial, notice-driven sanctions. That system includes cancellation of domain names for "pirate sites" about which right holders complain.[6] Through these contractual modifications, ICANN has abetted the development and implementation of a potentially large-scale program of privately-ordered online content regulation in the Internet's new generic Top Level Domains (new gTLDs).[7]

---

3. *See, e.g.*, *About Copyright Infringement*, ICANN, https://www.icann.org/resources/pages/copyright-2013-05-03-en (last visited Sept. 20, 2017) ("Complaints regarding copyright infringement due to Internet and website content are outside of ICANN's scope and authority.") (on file with the Washington and Lee Law Review).

4. *Id.*

5. *See, e.g.*, MOTION PICTURE ASS'N OF AM., INC., COMMENTS IN RESPONSE TO THE REQUEST OF THE UNITED STATES PATENT AND TRADEMARK OFFICE FOR PUBLIC COMMENTS: VOLUNTARY BEST PRACTICES STUDY 72 (Aug. 21, 2013), https://web.archive.org/web/20170706040417/https://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf (arguing that "all players in the Internet ecosystem," including "the various intermediaries that facilitate online commerce and speech . . . must play a meaningful role in addressing the problem of rampant piracy on the Web"); *see also* RECORDING INDUS. ASS'N OF AM., INC., COMMENTS IN RESPONSE TO THE REQUEST OF THE UNITED STATES PATENT AND TRADEMARK OFFICE FOR PUBLIC COMMENTS: VOLUNTARY BEST PRACTICES STUDY 15 (Aug. 19, 2013), https://web.archive.org/web/20170706040417/https://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf (asserting that "all responsible stakeholders in the Internet ecosystem . . . have a role to play in . . . deterring illegal activity").

6. *See infra* Part IV.B (explaining how ICANN's standard contracts provide the supporting legal infrastructure for the system).

7. "The early DNS included eight generic top-level domains (gTLDs): .edu (institutions of higher education—most of which were based in the United States), .gov (U.S. government), .mil (U.S. military), .com (commerce), .net (network resources), .org (other organizations and persons), .int (international treaty organizations), and .arpa (network infrastructure)." SIGNPOSTS, *supra* note 2, at 45. These are generally referred to as the "legacy gTLDs" to distinguish them from

This Article maps ICANN's ambivalent drift into online content regulation through its contractual facilitation of a "trusted notifier" copyright enforcement program between the Motion Picture Association of America (MPAA) and two registry operators for new gTLDs, Seattle-based Donuts and Abu Dhabi-based Radix.[8] For domain name registrants, who are the target of this new—and wholly unregulated—enforcement program, and for members of the public who worry about increasing online censorship, the development is cause for concern.

After discussing ICANN's history, mission, and circumscribed role in the resolution of disputes over trademarks in domain names, this Article reckons both descriptively and normatively with the fact that registry operators are now acting—without precedent but with ICANN's blessing—as private copyright enforcers on behalf of right holders.[9] My focus here is a program that is currently limited to alleged copyright violations; the program is designed, however, to flexibly address a wide range of activity that a wide range of notifiers might consider illegal or abusive.[10] Copyright may simply be the first-use case for what is

---

"new gTLDs." Since 2013, ICANN has greatly expanded the gTLD name space to include more than 1,000 "new gTLDs." *See* Akram Atallah, *A "Grand" Milestone: New gTLD Program Reaches 1,000th Delegation*, ICANN (May 25, 2016), https://www.icann.org/news/blog/a-grand-milestone-new-gtld-program-reaches-1-000th-delegation (last visited Sept. 10, 2017) ("There are nearly 50 times as many gTLDs as there were in 2013 when the first four applications completed the New gTLD Program.") (on file with the Washington and Lee Law Review).

8. *See* PRESS RELEASE, MPAA, DONUTS & THE MPAA ESTABLISH NEW P'SHIP TO REDUCE ONLINE PIRACY 1 (Feb. 9, 2016), http://www.mpaa.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf ("Under the terms of the agreement, the MPAA will be treated as a 'Trusted Notifier' for the purpose of reporting large-scale pirate websites that are registered in a domain extension operated by Donuts.") (on file with the Washington and Lee Law Review); *see also* Dean Marks, *MPAA/Radix Partnership Highlights Momentum Behind Voluntary Initiatives*, MPAA BLOG (May 13, 2016), http://www.mpaa.org/new-mpaaradix-partnership-highlights-the-continuing-momentum-of-voluntary-initiatives/#.V8cQ4TV76Hw (last visited Sept. 10, 2017) ("Similar to the partnership with Donuts announced in February, the MPAA will be treated as a 'trusted notifier' under this agreement.") (on file with the Washington and Lee Law Review).

9. *See infra* Parts IV–V (explaining ICANN's historical and evolving role in the enforcement of intellectual property rights through the DNS).

10. *See infra* Part IV.C (describing the program's broad conceptions of "trusted notifier" and "abusive behavior").

intended to become a broad program of notice-driven, registry-brokered domain takedowns.

II. ICANN 101

ICANN was formed as a private-sector, non-profit corporation in 1998 to manage the newly-invented DNS under contract with the U.S. Department of Commerce.[11] The organization has grown in size and structural complexity over time, but its *raison d'être* remains performance of the Internet's IANA (Internet Assigned Numbers Authority) functions.[12] These are, as ICANN describes them, "key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS)."[13] Stated succinctly, ICANN is responsible for ensuring that the DNS, as technical infrastructure, works stably and securely so that users' web page queries and email messages are routed to the correct servers.[14] ICANN's mandate is technical and administrative; it has not historically included enforcement of national or international law governing the content that is disseminated over the Internet.[15]

In 2016, in recognition of the increasingly international character and reach of the Internet, ICANN became a fully independent entity accountable only to its community of volunteer stakeholders.[16] The corporation is headed by a board of directors,

---

11. *See* SIGNPOSTS, *supra* note 2, at 77 (describing the founding of ICANN).

12. *See Welcome to ICANN!*, ICANN, https://www.icann.org/resources/pages/welcome-2012-02-25-en (last visited Sept. 20, 2017) ("[T]he Internet Corporation for Assigned Names and Numbers (ICANN) helps coordinate the Internet Assigned Numbers Authority (IANA) functions . . . .") (on file with the Washington and Lee Law Review).

13. *Id.*

14. *See id.* (describing the IANA functions in more detail).

15. *See What Does ICANN Do?*, ICANN, https://www.icann.org/resources/pages/what-2012-02-25-en (last visited Sept. 19, 2017) ("ICANN doesn't control content on the Internet . . . . ICANN's role is to oversee the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another.") (on file with the Washington and Lee Law Review).

16. Republican legislators failed in an eleventh-hour attempt to block the so-called IANA transition, and the DOC allowed its contract with ICANN to expire, according to plan, on September 30. *See* Paul Blake, *US Government*

which has sixteen voting members and five non-voting liaison representatives.[17] Having relinquished its historical role as ICANN's overseer, the United States is now a coequal member of ICANN's multilateral Governmental Advisory Committee (GAC), which represents the interests of national governments and a limited range of other entities.[18] The GAC is just one of many stakeholder groups that advise ICANN's board on matters of policy, but it is now substantially more influential than it was in ICANN's early days.[19]

ICANN's bureaucracy is notoriously byzantine, consisting of scores of advisory committees, supporting organizations, standing committees, working groups, review teams, and task forces.[20] All of these are known by acronyms that are a part of an ICANN-specific vernacular that insiders speak fluently.[21] For the uninitiated, understanding conversations about ICANN's

---

Hands Internet's 'Address Book' to International Organization, ABC NEWS (Oct. 1, 2016, 7:21 AM), http://abcnews.go.com/Business/us-government-hands-internets-address-book-international-organization/story?id=42474458 (last visited Sept. 19, 2017) ("Sen. Ted Cruz, R-Texas, was so alarmed by the transition that he attempted to have it blocked through a spending bill that was passed this week to keep the government funded beyond Friday.") (on file with the Washington and Lee Law Review).

17. ICANN, BEGINNER'S GUIDE TO PARTICIPATING IN ICANN 5 (2013) https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf [hereinafter BEGINNER'S GUIDE].

18. *See id.* at 11 ("The GAC's key role is to provide advice to ICANN on issues of public policy, especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements.").

19. *See* Jonathan Weinberg, *Governments, Privatization, and "Privatization": ICANN and the GAC*, 18 MICH. TELECOMM. TECH. L. REV. 189, 216 (2011) (describing the GAC's increasingly aggressive role in ICANN policy making on behalf of the U.S. and European governments and "their most influential business lobbies"); *see also* A. Michael Froomkin, *Almost Free: An Analysis of ICANN's 'Affirmation of Commitments*,' 9 J. ON TELECOMM. & HIGH TECH. L. 187, 195–96 (2011) [hereinafter Froomkin, *Almost Free*] (discussing causes and effects of 2002 changes to ICANN's bylaws that gave the GAC more power within ICANN's governance process).

20. *See Groups*, ICANN, https://www.icann.org/resources/pages/groups-2012-02-06-en (last visited Sept. 19, 2017) (listing the various entities which collectively form ICANN) (on file with the Washington and Lee Law Review).

21. For a detailed discussion of ICANN's highly complex structure and governance, see Emily M. Weitzenboeck, *Hybrid Net: The Regulatory Framework of ICANN and the DNS*, 22 INT'L J.L. & INFO. TECH. 49, 50 (2014).

structure and internal operations almost literally requires a translator. Put another way, informational barriers to entry in the ICANN universe are relatively high, and ICANN is consequently poorly understood by anyone whose curiosity about it is only casual or shallow.[22]

ICANN describes itself as an organization that makes policy for the DNS through a bottom-up, consensus-based, community governance process open to participation by anyone with time and inclination to volunteer.[23] In theory, ICANN's multi-stakeholder governance model is non-hierarchical and highly pluralistic.[24] As a practical matter, well-funded and organized interest groups, including trade associations representing corporate intellectual property right holders, have resources and capacity to participate that most individuals and public interest groups lack.[25] ICANN holds week-long meetings three times a year in different geographic regions, which means that in-person participation requires not only time and inclination, but also a significant financial investment in international travel.[26] Moreover,

---

22. *See* CECILIA TESTART, UNDERSTANDING ICANN'S COMPLEXITY IN A GROWING AND CHANGING INTERNET 28 (Apr. 15, 2014), https://poseidon01.ssrn.com/delivery.php?ID=607074089082020068021113094005072100019000031052064056118110009085029077069118126076045022127062105116060076100123002079083064105018000043039099127108110028115010123003044033107029077099020080028097018115098108117120010097025088066022025097067025096001&EXT=pdf (attributing the organization's opacity in part to the constant, voluminous flow of information and reports produced by its constituent groups and the poor organization of that information on ICANN's website).

23. *See* BEGINNER'S GUIDE, *supra* note 17, at 2 ("This decentralized governance model places individuals, industry, non-commercial interests and government on an equal level. Unlike more traditional, top-down governance models, where governments make policy decisions, the multistakeholder approach used by ICANN allows for community-based consensus-driven policy-making.").

24. *See id.* (stating that the goal of ICANN's governance model is to "mimic the structure of the Internet itself—borderless and open to all").

25. *See* LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 16 (2014) ("The question is not whose voices are *allowed* to participate but whose voices are *able* to participate. Technocracy and democracy often diverge, even when governance processes embody values of openness and inclusion.").

26. *See* BEGINNER'S GUIDE, *supra* note 17, at 3 ("Meetings are open to everyone and registration is free, but you are responsible for your own travel and lodging.").

commercial actors like the MPAA and the Recording Industry Association of America (RIAA), which belong to ICANN's Intellectual Property Constituency (IPC), are savvy lobbyists who know how to work the internal politics of governance to amplify their voices and draw the focus of leadership—including the increasingly influential GAC—to their concerns.[27] That is, after all, their job. The less sophisticated and economically powerful stakeholders within ICANN enjoy comparatively less access and influence.[28]

Given the size of the Internet, and the increasing size of its domain name space, coordinating the end-to-end operation of the DNS is no small task.[29] Beginning in 2013, ICANN created over 1,200 new gTLDs in the DNS.[30] The number of domain names that can be registered in these new gTLDs is vast. The importance of the IANA functions to the navigational security, speed, and reliability that users have come to expect of the Internet is difficult to overstate.[31] Even as online traffic becomes less browser- and email-centric, ICANN continues to exercise significant power

---

27. *Cf.* Weinberg, *supra* note 19, at 209 (discussing the rise of the GAC as a strong force within ICANN for making "broad arguments reflecting the views of private lobbies on a wide range of matters," including intellectual property protection).

28. *See id.* at 217 ("It has always been the case at ICANN that pressure by those with influence and power gets results.").

29. As a reference point, in 2016 there were over 130.6 million registered domain names in .com alone, though it is by far the largest of the gTLDs. *See .com Monthly Registry Reports*, ICANN, https://www.icann.org/resources/ pages/com-2014-03-04-en (last visited Sept. 19, 2017) (listing total domains registered in .com for the reporting period) (on file with the Washington and Lee Law Review); *see also Usage of Top Level Domains for Websites*, W3TECHS, https://w3techs.com/technologies/overview/top_level_domain/all (last visited Sept. 19, 2017) (reporting that 47% of all websites have .com domain names) (on file with the Washington and Lee Law Review).

30. *See Program Statistics*, ICANN, https://newgtlds.icann.org/en/program-status/statistics (last visited Sept. 19, 2017) (providing an overview of and statistics for the new gTLD program) (on file with the Washington and Lee Law Review); s*ee also* Atallah, *supra* note 7 (discussing the growth of the gTLD name space over time).

31. *See* SIGNPOSTS, *supra* note 2, at 18 ("The preservation of a stable, reliable, and effective Domain Name System [is] crucial both to effective Internet navigation and to the operation of the Internet and most of the applications that it supports.").

through its stewardship of the IANA functions. It controls which domains on the web are visible—or invisible, as some would like—to Internet users all over the world.[32]

III. Trademarks, Cybersquatting, and the UDRP

ICANN was not created or intended to be an intellectual property enforcer but was drawn from its inception into disputes over trademark rights in domain names.[33] As the Internet's commercial potential became clear in the mid-1990s, and established brick-and-mortar businesses began to appreciate the need for an online presence, some of the country's most famous corporations found themselves tangling with a new breed of entrepreneur. So-called cybersquatters were named for their practice of preemptively registering domain names containing famous trademarks and then offering to transfer the registrations to later-arriving trademark holders for exorbitant prices.[34] Dennis Toeppen, one of the early Internet's more prolific cybersquatters, registered over a hundred domain names containing famous trademarks for a range of businesses, including airlines (Delta, Lufthansa) and clothing retailers (Eddie Bauer, Neiman Marcus).[35] Cybersquatting was among the Internet's first cottage industries, and trademark holders did not like it.[36]

---

32. *See* Froomkin, *Almost Free*, *supra* note 19, at 211 ("ICANN can make visible and usable—or nearly invisible and largely useless—TLDs such as .com or .ibm.").

33. *See Timeline*, *supra* note 1 (describing the early formation of a dispute resolution process for domain names containing trademarked words and phrases) (on file with the Washington and Lee Law Review).

34. *See* Shields v. Zuccarini, 254 F.3d 476, 481 (3d Cir. 2001) (defining cybersquatting as "the bad faith, abusive registration and use of the distinctive trademarks of others as Internet domain names, with the intent to profit from the goodwill associated with those trademarks").

35. *See* Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1319 (9th Cir. 1998) ("Toeppen has registered domain names for various other companies including Delta Airlines, Neiman Marcus, Eddie Bauer, Lufthansa, and over 100 other marks. Toeppen has attempted to 'sell' domain names for other trademarks such as intermatic.com to Intermatic, Inc. for $10,000 and americanstandard.com to American Standard, Inc. for $15,000.").

36. *See id.* at 1317 ("Panavision accuses Dennis Toeppen of being a 'cyber

At the time, the practice was not obviously illegal, and courts across the country were struggling to apply brick-and-mortar trademark law in the uncharted territory of "cyberspace."[37] Their task was not an easy one because, as Michael Froomkin pointed out at the time, "[t]rademark law is organized around a set of objectives and assumptions that map badly onto the Internet."[38] Trademark rights in real space are linked to specific categories of goods and specific geography, meaning that businesses selling different types of goods in the same physical location—or the same type of goods in different physical locations—can legitimately use the same mark or similar marks.[39] The domain name space, by contrast, imposes scarcity inasmuch as a domain name in any given Top Level Domain (TLD) can be controlled by only one person.[40] So, while there can be multiple legitimate users of a trademark, there can be only one registrant for the corresponding domain name in any given TLD.[41] The potential for good faith legal conflicts arising from this technical limitation is obvious.

Cybersquatting, however, did not involve competing claims to a domain name by existing terrestrial businesses legitimately selling goods under the same trademark or similar trademarks.[42] To many, the practice looked opportunistic at best and extortionate at worst.[43] Powerful trademark holders were incensed at the

---

pirate' . . . .").

37. *See* Jennifer Golinveaux, *What's in a Domain Name: Is "Cybersquatting" Trademark Dilution?*, 33 U.S.F. L. REV. 641, 671 (1999) (critiquing courts' application of the trademark dilution doctrine in cybersquatting).

38. A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy"—Causes and (Partial) Cures*, 67 BROOK. L. REV. 605, 608 (2002) [hereinafter Froomkin, *Causes and (Partial) Cures*].

39. *See id.* at 614 (explaining that "the guiding principle behind much of trademark law is that it best achieves its purposes by limiting the reservation of rights in a name to the type of goods and location where those goods are sold").

40. *See id.* at 615 ("In contrast to trademark law's ability to tolerate multiple users of the same mark, the Internet enforces a greater degree of uniqueness.").

41. One impetus for adding new gTLDs to the domain name space was to eliminate this scarcity. TLDs could be geo-partitioned to solve the scarcity problem, but that would undermine the unitary and global nature of the DNS.

42. *See* Shields v. Zuccarini, 254 F.3d 476, 479–80 (3d Cir. 2001) (explaining the practice of a cybersquatter who registered five domain names that were similar to the plaintiff's legitimate domain name).

43. *See id.* at 487 (describing one cybersquatter's conduct as "egregious").

prospect of having to ransom domain names containing their marks from third parties whose sole motive for registration was resale of the domain name for profit.[44] Right holders persuaded policy makers, at least with respect to the practice of cybersquatting, that the right to control the use of a trademark in real space should translate into a right to control the use of a domain name containing that trademark. In 1999, Congress amended the Lanham Act to include the Anticybersquatting Consumer Protection Act (ACPA), creating a cause of action in federal courts for bad-faith registration of a domain name containing a protected trademark.[45]

ICANN almost simultaneously adopted the UDRP, driven by recommendations from a World Intellectual Property Organization (WIPO) study initiated at the request of the Department of Commerce in response to complaints by trademark holders about perceived violations of their rights within the DNS.[46] Commentators at the time were split over whether the program was a good idea. Critics raised concerns about the lack of procedural fairness for registrants, the potential for reverse domain name hijacking by overreaching trademark holders, and the danger of arbitral bias linked to complainants' ability to forum shop among accredited arbitrators.[47] Trademark holders were also

---

44. *See* Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1319 (9th Cir. 1998) ("Panavision alleged that Toeppen was in the business of stealing trademarks, registering them as domain names on the Internet and then selling the domain names to the rightful trademark owners.").

45. *See* 15 U.S.C. § 1125(d)(1)(A)(i)–(ii) (2012)

> A person shall be liable in a civil action by the owner of a mark . . . if, without regard to the goods or services of the parties, that person . . . has a bad faith intent to profit from that mark . . . and registers . . . a domain name that . . . is identical or confusingly similar to that mark . . . .

46. *See* Froomkin, *Causes and (Partial) Cures*, *supra* note 38, at 612, 623 (showing WIPO's recommendations, which later became the basis for the UDRP); *see also* A. Michael Froomkin, *Semi-Private International Rulemaking: Lessons Learned from the WIPO Domain Name Process*, *in* REGULATING THE GLOBAL INFORMATION SOCIETY 211, 212 (Christopher T. Marsden ed., 2000) (describing the "semi-private rulemaking" ICANN developed through input from WIPO). At the time, it was not clear what rights trademark holders *had* in the DNS, but they proceeded from the assumption that their territorial entitlements could and should translate straightforwardly into virtual ones.

47. *See* Froomkin, *Causes and (Partial) Cures*, *supra* note 38, at 688–710

unhappy, believing that the scope of the program was too narrow because it defined cybersquatting to require both bad faith registration and use, and because it excluded both claims for infringement beyond cybersquatting and claims for dilution.[48] From a doctrinal perspective, the UDRP effectively globalized what had previously been only national trademark rights by importing them into the boundary-agnostic DNS.[49] It was, in that sense, a major win for big-brand trademark holders.

The UDRP is an ICANN-administered alternative dispute resolution system in which ICANN-accredited arbitrators decide disputes via a streamlined, web-enabled process.[50] It is mandatory for all registrars and registrants in all gTLDs.[51] The UDRP was specifically designed to be ICANN's efficient, low-cost answer to cybersquatting, defined as "registration and use in bad faith" of a domain name that is identical or confusingly similar to a trademark.[52] Trademark cases that do not involve cybersquatting cannot be adjudicated via the UDRP—meaning, for example, that trademark claims against website operators who are alleged to sell

---

(discussing and suggesting solutions to a range of problems related to fairness).

48. *Id.* at 611. Froomkin collects citations to journal articles from the period that establish positions for and against the UDRP. *See id.* at 609 n.9, 610 n.10 (providing sources arguing from both sides of the UDRP debate).

49. *See id.* (observing that the UDRP effectively internationalized trademark law).

50. *See Domain Name Dispute Resolution Service for Generic Top-Level Domains*, WIPO, http://www.wipo.int/amc/en/domains/gtld/ (last visited Sept. 19, 2017) ("In December 1999, the WIPO Arbitration and Mediation Center began offering domain name dispute resolution services under the Uniform Domain Name Dispute Resolution Policy (UDRP).") (on file with the Washington and Lee Law Review).

51. *See Uniform Domain-Name Dispute-Resolution Policy*, ICANN, https://www.icann.org/resources/pages/help/dndr/udrp-en (last visited Sept. 19, 2017) ("All registrars must follow the Uniform Domain-Name Dispute-Resolution Policy . . . .") (on file with the Washington and Lee Law Review). The UDRP is not mandatory for managers of country code TLDs (ccTLDs), which are not administered by ICANN. *See FAQs*, ICANN, https://www.icann.org/resources/pages/faqs-2014-01-21-en (last visited Sept. 19, 2017) ("ICANN does not accredit registrars or set registration policies for ccTLDs.") (on file with the Washington and Lee Law Review).

52. *Uniform Domain Name Dispute Resolution Policy*, ICANN, https://www.icann.org/resources/pages/policy-2012-02-25-en (last visited Sept. 20, 2017) (on file with the Washington and Lee Law Review).

counterfeit branded goods (e.g., NFL jerseys or COACH handbags) are beyond its scope.[53] The UDRP's remedial scope is also narrow; its only available remedy is cancellation or transfer of the disputed domain name from the registrant to the complainant.[54]

Once a UDRP complaint is filed by a complainant (who can choose from a list of ICANN-approved providers), a registrant must participate in the UDRP process until its conclusion.[55] If either party to a UDRP proceeding is dissatisfied with the result, that party can file a claim contesting the result in a court of competent jurisdiction.[56] A losing registrant has only ten business days to file a claim in court and produce evidence that she has done so to the registrar.[57] If the registrant timely files a lawsuit, the prevailing complainant's remedy is stayed pending the outcome of the litigation.[58] If the losing registrant fails to file within the ten-day window, the domain name is cancelled or transferred.[59]

UDRP outcomes have historically skewed heavily in favor of complainants. WIPO reports that for all years the UDRP has been active, 86% of disputes have resulted in the transfer of the domain name to the complainant.[60] Registrants have prevailed in only 12%

---

53. *See id.* (explaining in section five that "[a]ll other disputes . . . that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding").

54. *See id.* (listing in section four that "[t]he remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant").

55. *See id.* ("The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).").

56. *Id.*

57. *Id.*

58. *See id.* ("[W]e will not implement the Administrative Panel's decision . . . until we receive . . . evidence satisfactory to us of a resolution; . . . evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or . . . a copy of an order from such court . . . .").

59. *See id.* ("We will then implement the decision unless we have received from you during that ten (10) business day period official documentation . . . .").

60. *Case Outcome (Consolidated): All Years*, WIPO, http://www.wipo.int/amc/en/domains/statistics/decision_rate.jsp?year= (last visited Sept. 19, 2017) (on file with the Washington and Lee Law Review).

of cases.[61] Critics of the process point to these numbers and to the fact that a small number of providers handle the vast majority of UDRP complaints as evidence that the system has created strong structural incentives for providers to rule in favor of complainants.[62] A provider whose results do not demonstrably favor complainants can easily find itself without any customers—as happened to eResolution, an accredited provider that went out of business in the early years of the UDRP for lack of a sustainable case load.[63]

The results of UDRP cases are undeniably wildly lopsided, but it is difficult to determine the extent to which pro-complainant bias is the cause. Empirical study of the quality of UDRP decision-making is hampered by the fact that opinions alone are published without any of the parties' submissions.[64] Lack of access to a full, public record makes it impossible to evaluate the provider's reasoning in light of the facts and competing arguments presented to it.[65] This lack of transparency—a longstanding general criticism of ICANN's culture—forecloses an important element of due process, namely the ability to interrogate and critique legal outcomes through examination of the inputs that informed them.

The UDRP became the anti-cybersquatting law of the global Internet because ICANN made it so, under significant pressure from trademark holders, through non-negotiable contractual provisions that flow down from ICANN to registries, then registrars, and ultimately registrants.[66] ICANN conditions the

---

61. *Id.*

62. *See* Orna Rabinovich-Einy, *The Legitimacy Crisis and the Future of Courts*, 17 CARDOZO J. CONFLICT RESOL. 23, 54 (2015) (summarizing criticisms of the UDRP).

63. *See* Froomkin, *Causes and (Partial) Cures*, *supra* note 38, at 718 ("Between the original submission of this Article and its going to press, eResolution folded, cited shrinking market share due to the complainants' bar's preference for providers they thought would enhance their chances of winning.").

64. *Id.* at 709.

65. *See id.* ("Not only does this make independent judgments difficult, but it makes any review by ICANN unlikely to be meaningful.").

66. *See* Froomkin, *Almost Free*, *supra* note 19, at 214 ("By requiring the registries—as a condition of being listed in the root—to require the registrars to include standard form terms in their contracts with registrants, ICANN gains a

accreditation of registrars on their agreement to require registrants to submit to the UDRP if a trademark holder disputes a registration on cybersquatting grounds.[67] Within this privately ordered legal framework, a registrant cannot register a domain name and have it entered into the authoritative zone file for the TLD to which it belongs unless the registrant agrees to submit to the UDRP.[68] In this way, trademark holders are indirect beneficiaries of ICANN's agreements with DNS intermediaries.

IV. Notice and Takedown in the New gTLDs

Starting with the launch of the new gTLDs, copyright holders appear to be laying the groundwork for a broad program of DNS-based enforcement, with the long-term goal of implementing a UDRP-like procedure for claims of piracy and counterfeiting that are wholly unrelated to any bad-faith or confusing use of domain names.[69] The idea of a UDRP for online copyright disputes has

---

degree of control over registrants . . . ."). The UDRP is not mandatory, however, for registrants of domain names in country code Top Level Domains (ccTLDs) (e.g., .ca, .fr, .nz). *See Uniform Domain Name Dispute Resolution Policy*, *supra* note 52 (stating that only some ccTLDs participate in the UDRP program).

67. *See* ICANN, REGISTRAR ACCREDITATION AGREEMENT § 3.8 (2013), https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf [hereinafter REGISTRAR ACCREDITATION AGREEMENT] ("During the Term of this Agreement, Registrar shall have in place a policy and procedures for resolution of disputes concerning Registered Names."). With the introduction of the new gTLDs, ICANN introduced an additional procedure for adjudicating cybersquatting complaints, the Uniform Rapid Suspension (URS) program. *See* ICANN, UNIFORM RAPID SUSPENSION § 1.2.6.1 (2013), http://newgtlds.icann.org/en/applicants/urs/procedure-01mar13-en.pdf [hereinafter URS] ("The Form Complaint shall include space for . . . [a]n indication of the grounds upon which the Complaint is based . . . , namely: . . . that the registered domain name is identical or confusing similar to a word mark . . . ."). A discussion of the URS is beyond the scope of this project. Participation in both the UDRP and the URS procedure is required under the 2013 Registrar Accreditation Agreement. REGISTRAR ACCREDITATION AGREEMENT, *supra*, § 3.8.

68. *See Uniform Domain Name Dispute Resolution Policy*, *supra* note 52 ("This Uniform Domain Name Dispute Resolution Policy (the 'Policy') . . . is incorporated by reference into your Registration Agreement . . . .").

69. *See* MEETING TRANSCRIPT, MARRAKECH—INDUSTRY BEST PRACTICES—THE DNA'S HEALTHY DOMAINS INITIATIVE 12–13 (Mar. 6, 2016), https://meetings.icann.org/en/marrakech55/schedule/wed-dna-healthy-domains-initiative/transcript-dna-healthy-domains-initiative-09mar16-en.pdf

been floating around in law reviews and journals for a long time, but it has never really gotten much traction.[70] With buy-in from new gTLD registry operators like Donuts and Radix, however, that status quo shows signs of changing.[71]

For its part, ICANN is walking the finest of lines with respect to involvement in copyright policing. As I explain below in Part B, ICANN created the legal infrastructure for the MPAA's trusted notifier program through specific provisions in its contracts with new gTLD intermediaries.[72] At the same time, however, it continues to insist that it is not in the business of online content regulation.[73] ICANN's apparent ambivalence on this point grows

---

[hereinafter MEETING TRANSCRIPT] ("We're discussing and exploring the idea that there could be a clearinghouse that can include copyright, piracy, and counterfeiting, along with other potential online abusive behavior, and then perhaps developing a new dispute resolution model similar to UDRP.").

70. *See, e.g.*, Steven Tremblay, *The Stop Online Piracy Act: The Latest Manifestation of a Conflict Ripe for Alternative Dispute Resolution*, 15 CARDOZO J. CONFLICT RESOL. 819, 820 (2014) ("Alternative dispute resolution . . . mechanisms provide a viable alternative to the costly and often counterproductive international efforts to curb online piracy."); *see also* Mark A. Lemley & Anthony R. Reese, *A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes*, 23 CARDOZO ARTS & ENT. L.J. 1, 1 (2005) ("In this article, we explain how such a dispute resolution system might work and propose a draft amendment to the Copyright Act to implement this system, with annotations to highlight some of the issues our proposal raises."); Andrew Christie, *The ICANN Domain-Name Dispute Resolution System as a Model for Resolving Other Intellectual Property Disputes on the Internet*, 5 J. WORLD INTELL. PROP. 105, 105 (2002) ("There is no reason why . . . the availability of this remedy need be limited to the type of conduct currently prohibited in the UDRP . . . .").

71. As this Article entered the editorial process, the Public Interest Registry, which operates the .org (legacy) TLD, announced that it plans to adopt a "Copyright Alternative Dispute Resolution Policy" in cooperation with the Healthy Domains Initiative. *See* Kevin Murphy, *The Pirate Bay Likely to Be Sunk as .org Adopts "UDRP for Copyright,"* DOMAIN INCITE (Feb. 8, 2017, 4:29 PM), http://domainincite.com/21517-the-pirate-bay-likely-to-be-sunk-as-org-adopts-udrp-for-copyright (last visited Sept. 20, 2017) ("Under its Healthy Domains Initiative, the DNA is proposing a Copyright Alternative Dispute Resolution Policy that would enable copyright holders to get piracy web sites shut down.") (on file with the Washington and Lee Law Review). The specific terms of that policy lie beyond the scope of this project. The Healthy Domains Initiative, which is applying significant pressure on DNS operators in all TLDs to go this route, is discussed in Part IV.A.

72. *See infra* Part IV.B (explaining the relevant ICANN contract provisions).

73. *See* Allen R. Grogan, *ICANN Is Not the Internet Content Police*, ICANN (June 12, 2015), https://www.icann.org/news/blog/icann-is-not-the-internet-

out of deep divisions within the stakeholder community—and, by extension, within ICANN's leadership—over the scope of ICANN's mission as the internet evolves.[74] The organization is struggling to find a way to answer right holders' demands without running afoul of its limited technical role. That may be an impossible compromise to strike, however.

Concern that ICANN is stepping onto a slippery slope by trying to accommodate copyright holders is legitimate. The more ICANN shows itself to be open to the idea that DNS intermediaries are appropriate content regulators, the more categories of content those intermediaries will likely be pressured to regulate. For example, many governments want ICANN, through DNS intermediaries, to help law enforcement police content that is unlawful under local law, including blasphemy, hate speech, and child pornography.[75] Their requests raise difficult questions about Internet jurisdiction and extraterritoriality that ICANN is not in a position to resolve, given its narrow technical mandate.[76] The brouhaha over copyright is, in the end, a microcosm of a broader

---

content-police (last visited Sept. 20, 2017) ("Allow me to say this clearly and succinctly—ICANN is not a global regulator of Internet Content . . . .") (on file with the Washington and Lee Law Review). Significantly, ICANN did not mandate any protocol for copyright or anti-counterfeiting enforcement in the new gTLDs when it required new gTLD intermediaries to adopt the URS procedure for cybersquatting.

74. *See* Shane Tews, *3 Strategies for Keeping ICANN and IANA on Mission and out of Politics*, TECHPOLICYDAILY (Sept. 10, 2015, 6:00 AM), https://web.archive.org/web/20160312155239/http://www.techpolicydaily.com/internet/icann-and-iana-on-mission/ (last visited Sept. 20, 2017) ("[C]an ICANN be trusted to be a good steward of the Internet's future?") (on file with the Washington and Lee Law Review).

75. *See* Grogan, *supra* note 73 (describing the range of online content that some government stakeholders would like to have ICANN play a role in censoring); MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 197 (2010) ("More governments and censorship advocates have begun to think that blocking or 'filtering' techniques [within the DNS] could recreate the kind of control they once had over traditional territorial media.").

76. *See* MUELLER, *supra* note 75, at 201 ("A true 'technical coordinator' role implies that ICANN would be indifferent to any social goals other than its fundamental one of maintaining the global uniqueness of domain names . . . . This implies neutrality with respect to social outcomes unrelated to that basic mission.").

struggle within ICANN over the purpose and direction of the newly independent organization.

A. The Background: From Congress to ICANN

Right holders' anti-piracy aspirations for the DNS entered the public's consciousness in 2011 with a notorious piece of failed legislation called the Stop Online Piracy Act (SOPA).[77] Through SOPA, copyright holders sought to expand enforcement of their rights into the DNS (among other online systems, including payment systems and advertising networks).[78] The bill authorized the Attorney General to obtain court orders compelling ISPs operating non-authoritative domain name servers[79] to block access to "foreign infringing sites" by disrupting the normal technical

77. Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011). The ideas underlying SOPA had been percolating in policy circles, through entertainment industry proxies, as early as 2009. *See, e.g.*, DANIEL CASTRO, RICHARD BENNETT & SCOTT M. ANDES, THE INFO. TECH. & INNOVATION FOUND., STEAL THESE POLICIES: STRATEGIES FOR REDUCING DIGITAL PIRACY 3 (2009), http://www.itif.org/files/2009-digital-piracy.pdf (promoting site blocking "at the ISP level"). In 2010, a bill called COICA, which contained provisions similar to those that later appeared in SOPA, was introduced in the Senate but failed to advance. *See* Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. (2010) (seeking to create enforcement mechanisms against "rogue websites").

78. *See* Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523, 1540–42 (2015) (explaining SOPA's DNS blocking provisions).

79. A non-authoritative domain name server, sometimes called a "caching server," is one that stores a cache of all domain name lookup requests for which it has received a response from a registry-maintained authoritative domain name server in the past. *See* DANIEL KARRENBERG, THE INTERNET DOMAIN NAME SYSTEM EXPLAINED FOR NON-EXPERTS 2 (2004), https://www.internetsociety.org/internet-domain-name-system-explained-non-experts-daniel-karrenberg ("Your computer knows the address of a nearby DNS 'caching server' and will send the query there."). Residential and commercial broadband providers (ISPs) operate caching name servers to respond efficiently to their subscribers' queries. *Id.* Thanks to local caching servers, many DNS requests need never be routed through the actual infrastructure of the DNS, which decreases processing burdens on the system as a whole. *Id.* Authoritative domain name servers for TLDs are controlled by their respective registries. SIGNPOSTS, *supra* note 2, at 133. For each TLD, there are redundant authoritative domain name servers ("slave" servers), but there is a single primary ("master") server for that TLD. The master server stores the TLD's authoritative zone file—the database that links all domain names to their corresponding Internet Protocol (IP) addresses for navigational purposes. *Id.* at 90.

process by which domain names resolve to their underlying IP addresses.[80]

When SOPA unexpectedly—and spectacularly—sank, just as it seemed ready to sail through Congress, right holders turned their attention to ICANN, a forum below the radar of the powerful coalition of tech companies and grassroots organizations that had mobilized to defeat SOPA.[81] At the time, ICANN's new gTLD project was already underway.[82] In the mix were .movie and .music, "strings" of special interest to the MPAA and the RIAA.[83]

In ICANN's cycle of meetings involving the governance and roll out of the new gTLDs, the MPAA and the RIAA saw an opportunity to enhance ICANN's intellectual property

---

80. SOPA, *supra* note 77, at § 102. Under pre-existing law, a "domestic" domain name—meaning one registered in the United States—could be seized ex parte on a showing of probable cause to believe that the name was being used to facilitate criminal copyright infringement. *See* 18 U.S.C. § 2323 (2012) ("[I]n imposing sentence on a person convicted of an offense . . . shall order . . . that the person forfeit to the United States Government any property subject to forfeiture under subsection (a) . . . ."). SOPA would have expanded the field of DNS enforcement to reach activity on "foreign" sites—meaning those registered in and operated from jurisdictions outside the United States. I enclose the words domestic and foreign in quotation marks to highlight the fact that Internet names and addresses are purely logical and do not actually correspond to physical geography.

81. *See* Amy Goodman, *The SOPA Blackout Protest Makes History*, GUARDIAN (Jan. 18, 2012), https://www.theguardian.com/commentisfree/cifamerica/2012/jan/18/sopa-blackout-protest-makes-history (last visited Sept. 20, 2017) (reporting on the unprecedented breadth and scale of the public campaign to block SOPA from becoming law) (on file with the Washington and Lee Law Review).

82. *See New Generic Top-Level Domains: About the Program*, ICANN, https://newgtlds.icann.org/en/about/program (last visited Sept. 19, 2017) (explaining the history of the new gTLD program) (on file with the Washington and Lee Law Review).

83. ICANN delegated .movie, meaning it assigned responsibility for the new TLD to a registry and added it to the DNS Root Zone, in 2015. *New Generic Top Level Domains: Delegated Strings*, ICANN, https://newgtlds.icann.org/en/program-status/delegated-strings (last visited Sept. 19, 2017) (on file with the Washington and Lee Law Review). Delegation of .music has been complicated by the fact that ICANN received eight competing applications to control it, making it a "contested string." *New gTLD String Similarity Contention Sets*, ICANN, https://gtldresult.icann.org/application-result/applicationstatus/stringcontentionstatus (last visited Sept. 19, 2017) (on file with the Washington and Lee Law Review). When this article went to press, .music was still not delegated.

enforcement mandate to include non-judicial, DNS-based (and therefore global) remedies for copyright infringement.[84] MPAA and RIAA representatives, backed by the IPC, demanded that ICANN and its new gTLD contractors promote a "safe internet ecosystem" by enforcing their members' copyrights in films and music.[85]

A campaign for concerted, private anti-piracy enforcement within the DNS—branded the "Healthy Domains Initiative"—is being spearheaded with ICANN's approval[86] by the IPC and the recently launched Domain Name Association (DNA), a trade group that represents the interests of DNS intermediaries participating in the new gTLD program.[87] Donuts and Radix are both

---

84. *See* David Post, *ICANN, Copyright Infringement, and "the Public Interest,"* WASH. POST: VOLOKH CONSPIRACY (Mar. 9, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/03/09/icann-copyright-infringement-and-the-public-interest/?utm_term=.2586b26c9234 (last visited Sept. 20, 2017) (reporting on the MPAA and RIAA's campaign to involve ICANN directly in copyright enforcement) (on file with the Washington and Lee Law Review). *Cf.* MUELLER, *supra* note 75, at 141 ("We are currently in a period . . . in which state and corporate advocates of intellectual property protection propose ever harsher and more systemic interventions into the ecology of information-communication technology . . . .").

85. Post, *supra* note 84; *see also* Letter from Victoria Sheckler, Deputy Gen. Counsel, RIAA, to Steve Crocker, Chairman of the Bd., ICANN, and Fadi Chehade, CEO, ICANN 1 (Mar. 5, 2015), https://www.icann.org/en/system/files/correspondence/riaa-to-icann-05mar15-en.pdf

> [O]ur overriding concerns are to ensure that the internet ecosystem is a safe, vibrant, and innovative place where legitimate music creation, access, and distribution can thrive. In light of this, we expect all in the internet ecosystem to take responsible measures to deter copyright infringement to help meet this goal.

(on file with the Washington and Lee Law Review).

86. The Healthy Domains Initiative ran a meeting alongside the 2016 ICANN meeting in Marrakesh, with ICANN's head of contractual compliance in attendance. *See* MEETING TRANSCRIPT, *supra* note 69, at 1 ("I'm Allen Grogan. I'm the Chief Compliance Officer at ICANN."). At an earlier meeting in Dublin, ICANN's leadership "encouraged a community discussion on establishing a voluntary framework to handle contractual obligations relating to content." BRIAN J. WINTERFELDT ET AL., FOUR KEY TAKEAWAYS FROM ICANN 54, at 5 (2015), https://www.mayerbrown.com/files/Publication/185ad1ed-e701-4be3-85a5-86a5ad97ad7a/Presentation/PublicationAttachment/a91bdeae-4f07-41c7-8b43-5fdd096223b5/151117-UPDATE-IP.pdf.

87. *See The Domain Name Association Launches Healthy Domains Initiative as Industry-Led Effort to Evolve Internet Naming Ecosystem*, PR NEWSWIRE (Feb. 16, 2016, 9:08 AM), http://www.prnewswire.com/news-releases/the-domain-name-association-launches-healthy-domains-initiative-as-industry-led-effort-to-

members.[88] The DNA's stated motivation for cooperation with right holders is to "appease . . . pressures" coming from "outside."[89] In its public-facing rhetoric, the DNA positions the trusted notifier program as "a positive example of self-governing."[90] What the DNA's characterization of the trusted notifier program obscures, however, is the fact that registrants—and not the registries themselves—are the ultimate regulatory targets of the program, which they played no part in shaping. For ICANN, describing the trusted notifier program as a form of voluntary "self-governance" for registries diverts attention from the uncomfortable fact that the program is, in fact, a new form of DNS governance that draws its legal force from ICANN's web of contracts with DNS intermediaries.[91]

Under the anodyne rubric of "Public Interest Commitments," the IPC successfully lobbied ICANN for the creation of a top-down contractual infrastructure for DNS intermediaries that supports a privately ordered system of copyright notice and takedown for entire second-level domains.[92] In short, right holders achieved

---

evolve-internet-naming-ecosystem-300220548.html (last visited Sept. 20, 2017) (listing participants in the HDI's first "summit") (on file with the Washington and Lee Law Review). According to the DNA's website, the organization's mission is "[t]o promote the interest of the domain name industry by advocating the use, adoption, and expansion of domain names as the primary tool for users to navigate the Internet." *What is the Domain Name Association?*, DOMAIN NAME ASS'N, http://www.thedna.org/what-is-the-domain-name-association/ (last visited Sept. 19, 2017) (on file with the Washington and Lee Law Review).

88. *List of Members*, DOMAIN NAME ASS'N, http://www.thedna.org/current-dna-members/ (last visited Sept. 19, 2017) (on file with the Washington and Lee Law Review).

89. MEETING TRANSCRIPT, *supra* note 69, at 3–4.

90. *The Domain Name Association Launches Healthy Domains Initiative as Industry-Led Effort to Evolve Internet Naming Ecosystem*, *supra* note 87.

91. *See* Weitzenboeck, *supra* note 21, at 54 ("Governance of the gTLD namespace is contractual, with a web of contracts spun between, respectively, ICANN, registries, registrars, data escrow providers and eventually between the registrants and the registrars with which they deal.").

92. *See The Domain Name Association Launches Healthy Domains Initiative as Industry-Led Effort to Evolve Internet Naming Ecosystem*, *supra* note 87 (explaining how the Public Interest Commitments, or PICs, came into existence); Letter from Steven J. Metalitz, Counsel for the Coal. for Online Accountability, to Goran Marby, Pres. and CEO of ICANN 1 (June 17, 2016), https://www.icann.org/en/system/files/correspondence/metalitz-to-marby-17jun16-en.pdf [hereinafter Letter from Metalitz to Marby] ("IPC considers these PIC

through ICANN as a matter of private ordering the site-blocking remedy for "pirate sites" in new gTLDs that they failed to get for all gTLDs through SOPA. The ICANN program may even be preferable from their point of view, because it requires no judicial intervention at all.[93]

B. ICANN's Legal Infrastructure for DNS-Based Copyright Enforcement

The trusted notifier program, unlike the UDRP, is not ICANN's program; however, ICANN laid the legal foundation for it through mandatory provisions in its contracts with DNS intermediaries—similar to those that make the UDRP binding on all registrants.[94] ICANN requires all registry operators for the new gTLDs to execute its 2013 ICANN-Registry Agreement, which contains a set of standard terms known as Specification 11—Public Interest Commitments.[95] One of the terms in Specification 11 is a pass-along, or flow-down, provision requiring registry operators to include in their contracts with registrars a provision requiring registrars to include in their contracts with registrants "a

---

obligations to be essential safeguards that must be vigorously enforced in order to promote the healthy development of the new gTLD namespace.") (on file with the Washington and Lee Law Review). The PICs provision is "Specification 11" in the ICANN Registry Agreement. ICANN, REGISTRY AGREEMENT § 2.17, Specification 11 (2013), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf (listing the public interest commitments in the Registry Agreement).

93. *See infra* Part C (describing the program's procedures, which are completely non-judicial).

94. *See* Froomkin, *Almost Free*, *supra* note 19, at 214

> By requiring the registries—as a condition of being listed in the root—to require the registrars to include standard form terms in their contracts with registrants, ICANN gains a degree of control over registrants, at least to the extent that a registrar could impose terms in a contract with the end-user. To date, ICANN has used this power only for matters ostensibly relating to trademark issues raised by domain name registrations, most notably its imposition of the Uniform Domain Name Process ("UDRP") . . . .

95. ICANN, REGISTRY AGREEMENT § 2.17, Specification 11 (2013), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.

provision prohibiting Registered Name Holders from . . . piracy, trademark or copyright infringement, . . . and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."[96] Through this provision, an express prohibition on copyright infringement and the identification of consequences for it are pushed down from ICANN to registry operators to registrars.[97]

The endpoint in this cascade of contractual obligations is, of course, the registrant, whose registration is conditioned on her acceptance of the prospect that her domain name may be suspended if she is found to have engaged in piracy or copyright infringement.[98] The flow-down provision raises a number of interpretive questions, however, to which the contract as a whole provides no clear answers. For example, who has the authority to determine whether a registrant has engaged in copyright infringement? A court of law? The registrar? A right holder complaining to the registrar? There is also ambiguity concerning the imposition of consequences. Does the provision create a duty or just a right on behalf of the registrar to impose consequences for infringement? What "applicable law" and "related procedures" does the provision contemplate as principles guiding or limiting the suspension of domain names?

Right holders have taken the position with ICANN that registrars have a contractual duty not only to *include* Specification 11's anti-infringement provision in their registration agreements, but also to *enforce* it by suspending registered domain names in response to right holder reports of "abuse."[99] The ICANN 2013

---

96. *Id.*

97. *See* Froomkin, *Almost Free*, *supra* note 19, at 214 (explaining how this structure works to bind registrants to the UDRP). Note that the inclusion of trademark infringement in the list of actionable activity under Specification 11 flies in the face of the UDRP's (and the URS's) limited scope for cybersquatting.

98. *See* ICANN, REGISTRY AGREEMENT § 2.17, Specification 11 (2013), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf (requiring "Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from . . . piracy . . . or copyright infringement" that would trigger "suspension of the domain name").

99. *See* Allen R. Grogan, *Community Outreach on Interpretation and Enforcement of the 2013 RAA (Registrar Accreditation Agreement)*, ICANN (June

Registrar Accreditation Agreement (RAA) requires registrars to maintain an "abuse contact" to receive "reports of Illegal Activity" involving domain names for which they provide services.[100] It further requires registrars to "take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse."[101] ICANN requires any registrar that wants to register domain names in new gTLDs to execute the 2013 version of the RAA.[102]

Reading the anti-infringement flow-down provision in Specification 11 together with the anti-abuse provision in the RAA, right holders have argued to ICANN's contractual compliance staff that registrars breach their obligations to ICANN if they fail to implement notice and takedown for domain names associated with alleged pirate sites.[103] As with the anti-infringement provision in Specification 11, however, the RAA's broad anti-abuse provision raises compliance questions to which the agreement as a whole provides no clear answers. What conduct on the part of a registrant or users of the registrant's website qualifies as "abuse"? What information must a "report" contain? What are "reasonable steps" for investigating a report of abuse or illegal activity? What does it mean for a registrar to "respond appropriately" to a right holder's report of illegal activity when the activity in question is merely alleged and not judicially proven? From the perspective of both registrars and registrants, these are critical questions.

Some registrars have taken the position that an appropriate response to an abuse complaint from a right holder is to inform the complainant that the registrar is not in a position to adjudicate the legality of a registrant's activity, and the complainant should

---

11, 2015), https://www.icann.org/news/blog/community-outreach-on-interpretation-and-enforcement-of-the-2013-raa (last visited Sept. 20, 2017) (explaining that "a number of parties submitting abuse reports believe that an appropriate response to illegal activity requires the registrar to suspend the registered name holder's domain name and requires ICANN to terminate the registrar's 2013 RAA (Registrar Accreditation Agreement) if the registrar fails to do so") (on file with the Washington and Lee Law Review).

100. REGISTRAR ACCREDITATION AGREEMENT, *supra* note 67, § 3.18.

101. *Id.*

102. *Id.*

103. *See* Grogan, *supra* note 99 (explaining the right holders' position).

therefore seek redress from competent legal authorities.[104] These registrars are unwilling to make substantive judgments about the legality of content accessible through domain names they have registered, opting to rely instead on valid legal process.[105]

ICANN's contractual compliance staff has found itself in the uncomfortable position of mediating the ongoing controversy over the legal effect of Specification 11 and its interaction with the anti-abuse provision in the RAA.[106] ICANN took an official position with respect to the controversy in a letter from the chair of the board of directors to the president of the IPC in the summer of 2016.[107] The letter affirmed that ICANN will enforce its contracts with DNS intermediaries, just not in the way that right holders would like:

> This does not mean, however, that ICANN is required or qualified to make factual and legal determinations as to whether a Registered Name Holder or a website operator is violating applicable laws and governmental regulations, and to assess what would constitute an appropriate remedy for such activities in any particular situation.[108]

Some members of the IPC have accused ICANN of "backtracking" on Specification 11 by failing to adopt a policy of terminating accreditation for both registrars that do not suspend registered domain names in response to right holder allegations of piracy and registries that do not require registrars to do so.[109]

---

104. *See id.* (explaining the position of unspecified registrars that a judicial determination of infringement may legitimately be regarded under the agreement as a reasonable precondition for suspension).

105. *Id.*

106. ICANN provides a formal means through its contractual compliance program for third parties to complain that an accredited DNS intermediary is not living up to its legal obligations to ICANN. For further discussion and examples of ICANN's contractual compliance procedures, see *Contractual Compliance*, ICANN, https://www.icann.org/resources/pages/compliance-2012-02-25-en (last visited Sept. 19, 2017) (on file with the Washington and Lee Law Review).

107. Letter from Stephen D. Crocker, Chair of the Bd., ICANN, to Greg Shatan, President, Intellectual Prop. Constituency 1 (June 30, 2016), https://www.icann.org/en/system/files/correspondence/crocker-to-shatan-30jun16-en.pdf [hereinafter Letter from Crocker to Shatan].

108. *Id.*

109. *See* Kevin Murphy, *Fight as ICANN "Backtracks" on Piracy Policing*, DOMAIN INCITE (July 1, 2016, 8:49 AM), http://domainincite.com/20692-fight-as-

On its face, Specification 11 mandates only that registrars *include* the anti-infringement provision in their registration agreements, not that they *interpret and enforce* the provision in the way that right holders demand.[110] As nonparties to both the RAA (between ICANN and registrars) and registrars' contracts with registrants, right holders have no standing to demand enforcement of either contract's terms.[111] To backstop this default rule of privity, ICANN's RAA contains an express provision stipulating that there are no third party beneficiaries to the agreement.[112] ICANN and its accredited registrars are thus insulated from breach of contract claims by right holders who might otherwise be inclined to test the meaning of Specification 11 and the anti-abuse provision in court.

ICANN's contractual compliance staff has so far supported registrars that elect not to treat right holder complaints of infringement as actionable proof of abuse or illegal conduct.[113] However, with the inclusion of the flow-down provision in Specification 11 of the ICANN-Registry agreement and the anti-abuse provision in the 2013 version of the RAA, ICANN has opened a Pandora's box with respect to content regulation that it may ultimately be unable to close, particularly in light of the IPC's power within ICANN.[114]

---

icann-backtracks-on-piracy-policing (last visited Sept. 20, 2017) ("New gTLD registries are not going to be held accountable for domains used for content piracy.") (on file with the Washington and Lee Law Review).

110. ICANN, REGISTRY AGREEMENT § 2.17, Specification 11 (2013), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.

111. *See* 13 WILLISTON ON CONTRACTS § 37:1 (4th ed.) (explaining the common law rule of privity and the exception for intended third-party beneficiaries).

112. *See* REGISTRAR ACCREDITATION AGREEMENT, *supra* note 67, § 7.5 ("This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this Agreement, including any Registered Name Holder.").

113. *See supra* notes 107–108 and accompanying text (explaining difficulties registrars face in "evaluating alleged violations of law").

114. Changes to ICANN's by-laws, for which the IPC successfully lobbied in 2016, may make it difficult going forward for ICANN to rely on its technical mission as a reason for holding the line on Crocker and Grogan's interpretation of Specification 11. *See* Letter from Metalitz to Marby, *supra* note 92, at 2

> Furthermore, the revisions to the ICANN by-laws that the Board

C. The MPAA's "Trusted Notifier" Program

As mentioned above, ICANN has been supportive of voluntary enforcement agreements between DNS intermediaries and right holders and has facilitated them through Specification 11 and the 2013 RAA.[115] While controversy swirls within ICANN over how to interpret those terms, Donuts and Radix agreed in the spring of 2016 to partner with the MPAA to implement a trusted notifier program covering all domain names in new gTLDs they control.[116] Donuts administers .movie in addition to hundreds of other gTLDs.[117] Radix is an applicant for .music, which ICANN has not yet delegated due to unresolved competing applications.[118] It seems all but certain, however, that Radix will add the RIAA to its roster of trusted notifiers if or when Radix gains control of .music.

According to a brief summary of the program publicly released by Donuts and the MPAA, a "trusted notifier" is defined very broadly as "an industry representative trade association that represents no single company, a recognized no[t]-for-profit public interest group dedicated to examining illegal behavior, or a similarly situated entity with demonstrated extensive expertise in the area in which it operates and ability to identify and determine the relevant category of illegal activity."[119] The document does not

---

> approved just last month explicitly enshrine ICANN's authority "to negotiate, enter into and enforce agreements, *including public interest commitments*," and specifically bar any party from challenging the PICs or other provisions of the new gTLD registry agreements "on the basis that such terms and conditions conflict with, or are in violation of, ICANN's Mission or otherwise exceed the scope of ICANN's authority or powers."

(emphasis added) (quoting Revised By-Laws, §§ 1.1.d.ii, iv).

115. *See, e.g.*, Letter from Crocker to Shatan, *supra* note 107, at 1–4 (stating that ICANN is both aware and supportive of the DNA's Healthy Domains Initiative and associated voluntary enforcement agreements).

116. Press Release, Radix & MPAA, Radix and the MPAA Establish New Partnership to Reduce Online Piracy (May 13, 2016), http://www.mpaa.org/wp-content/uploads/2016/05/Radix-and-the-MPAA-Establish-New-Partnership-to-Reduce-Online-Piracy.pdf (on file with the Washington and Lee Law Review).

117. *See Program Statistics*, *supra* note 30 (showing links to ICANN's official list of all delegated new gTLD strings).

118. *Id.*

119. CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM 1,

specify what makes any given group "recognized" for "examining illegal behavior" or what counts as "demonstrated extensive expertise" when it comes to qualifying as a trusted notifier.[120] Judgments about eligibility for trusted notifier status appear to be left to the discretion of the participating registry operator.

As an operational matter, the registry operator agrees to treat the trusted notifier's complaints "expeditiously and with a presumption of credibility."[121] "Expeditiously" means, "absent exceptional circumstances," that the "[r]egistry will coordinate with the applicable registrar" and render a final decision within ten business days of the complaint.[122] Notably, the registry has no obligation under the agreement to independently investigate the complaint before imposing a sanction, though it "may conduct its own investigation" if it is inclined to do so.[123]

The agreement outlines a workflow in which the notifier complains to the registry, the registry coordinates with the registrar, and "as appropriate" either the "registrar (or [r]egistry if registrar declines) may provide" the complaint to the registrant with a "reasonable deadline" for a response.[124] The "as appropriate" and "may provide" terms signal that the registrant

---

https://web.archive.org/web/20160615074509/http:/www.donuts.domains:80/images/pdfs/Trusted-Notifier-Summary.pdf.

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.* Remember, however, that the applicable registrar is obligated under the 2013 RAA to "investigate and respond appropriately to any reports of abuse." REGISTRAR ACCREDITATION AGREEMENT, *supra* note 67, § 3.18. So, even if the registrar is not a participant in the trusted notifier program, its obligations to ICANN require it to take action of some (unspecified) kind in response to third-party reports of abuse and illegal activity. As discussed in Part IV.B, not all registrars agree that the RAA requires them to impose sanctions on registrants in response to right holder complaints, absent a court order or other legal authority. ICANN has publicly backed these registrars' position, which means that registrars unwilling to act without a court order are a potential obstacle for notifiers who believe they're entitled to be "trusted." As an end run around uncooperative registrars, the trusted notifier agreement provides that the participating registry will simply take matters into its own hands if the applicable registrar declines to act. *See* CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM, *supra* note 119, at 2 (providing that the registry may impose sanctions "in its discretion" if it agrees with the notifier's assessment of the domain's legality).

124. CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM, *supra* note 119, at 2.

will not necessarily receive notice of the complaint or be given an opportunity to respond.[125] If the registrant does get the chance to respond, how much time is "reasonable" is an open question, but given the ten-day window for the registry's ultimate decision, the registrant's deadline must necessarily be a very short one—no more than a matter of a few days. For a registrant whose business is dependent on his or her active domain, such a short amount of time for a response strains the definition of reasonableness. And the consequences for failing to meet a registry's tight deadline are potentially final, because a registrant has neither a right to appeal the registry's adverse decision nor a claim for breach of contract against the registry.[126]

If the registry agrees with the notifier that "the domain clearly is devoted to abusive behavior," then "the [r]egistry, in its discretion, may suspend, terminate, or place the domain on registry lock, hold, or similar status."[127] Because the program does not require the registry to actually investigate the complaint or to solicit a response from the registrant, there is a high risk that participating registries will default to a rubber stamp approach. Indeed, the program is designed to have DNS intermediaries intrinsically trust and quickly execute the notifier's legal judgments. A registrant who disagrees with the registry's unilateral decision could try to seek redress from ICANN through its contractual compliance process, but that registrant would likely be rebuffed in the same way that right holders have been.[128]

D. The Trusted Notifier Program and the UDRP Compared

Unlike the UDRP, the trusted notifier program is ICANN-enabled but not ICANN-developed or -sponsored, meaning that participating registries and right holders were free to

---

125. *Id.*

126. A domain name registrant has no contractual relationship with a registry. The registrant's only DNS-relevant contractual relationship is with the registrar that registered the domain name.

127. CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM, *supra* note 119, at 2.

128. *Cf.* Letter from Crocker to Shatan, *supra* note 107, at 1–4 (disavowing a role for ICANN in content regulation).

negotiate a deal mutually agreeable to them, without vetting the terms through ICANN's multi-stakeholder policy development process.[129] With the trusted notifier program, ICANN has facilitated a program of private, DNS-based content regulation for which it now disclaims responsibility and oversight.[130]

The resulting set of procedures is loosely defined and heavily biased in favor of complainants. It altogether lacks uniform, substantive standards for determining what constitutes "clear and pervasive abusive behavior"[131] that will justify a registry in canceling or suspending a registrant's domain name. The publicly released document describing the program is completely generic with respect to what qualifies as actionable conduct. The program gives trusted notifiers an open invitation to provide a "[n]on-exhaustive [i]dentification of the law(s) being violated."[132] Surprisingly, given the copyright-specific nature of the MPAA's interests, the document makes no reference to copyright infringement at all—a worrying sign that copyright may simply be the thin edge of the wedge when it comes to notice-driven content regulation through the DNS. The UDRP, in contrast, begins and ends with cybersquatting, the elements of which the program's procedures clearly define.[133]

The UDRP and the trusted notifier program also differ significantly in terms of the nature and amount of information complainants must provide to initiate a claim. A trusted notifier's complaint can consist of little more than identification of a law allegedly being violated, a "clear and brief" description of how the site is violating the law, and evidence of illegality in the form of sample URLs and screen shots.[134] The UDRP, by contrast, requires

---

129. *See* MEETING TRANSCRIPT, *supra* note 69, at 2 ("To be clear, the Healthy Domains Initiative was a product of the DNA—not ICANN, not ICANN Contractual Compliance; we weren't involved in it—but it's an example of the kind of voluntary initiatives that I think can be constructive.").

130. *Id.*

131. CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM, *supra* note 119, at 2.

132. *Id.* at 1.

133. *See Uniform Domain Name Dispute Resolution Policy*, *supra* note 52 (defining applicable disputes and listing factors for determining bad faith registration and use of a domain name).

134. *See* CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM, *supra* note 119, at 1 (requiring the trusted notifier to provide a "[d]etailed description of the

a complainant to plead a case based on explicit, published factors for determining a narrowly defined category of wrongful conduct—bad faith registration and use of a domain name.[135]

The trusted notifier program also differs from the UDRP in that the UDRP guarantees the registrant an opportunity to respond and, if the outcome is unfavorable, to bring a claim for declaratory judgment in a court of competent jurisdiction.[136] An opportunity to respond and a right to appeal an adverse judgment are basic to fair process. They are especially necessary in a program like the trusted notifier program, which calls on registry employees with no particular expertise or training in the law to make domain-wide determinations about the legality of content under an unspecified range of laws from an unspecified range of jurisdictions, some of which may have conflicting laws on the same subject matter. The risk of error by inexpert decision-makers when so much content and so many legal variables are in play is obviously high.

For all its asserted shortcomings and intimations of pro-complainant bias, the UDRP is at least run by accredited legal professionals who are tasked with applying uniform legal standards neutrally to the cases before them.[137] Unlike registries

---

abusive activity (i.e., sample URLs, screen shots); [n]on-exhaustive [i]dentification of the law(s) being violated by the activity; and a [c]lear and brief description of why the site's activity violated the specified law(s)").

135. *See Rules for Uniform Domain Name Dispute Resolution Policy*, ICANN (Sept. 28, 2013), https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en (last visited Oct 12., 2017) (listing the required elements of a complaint) (on file with the Washington and Lee Law Review).

136. *See Uniform Domain Name Dispute Resolution Policy*, *supra* note 52 (providing that a registrant may file a lawsuit within 10 days of receiving an adverse result in a UDRP proceeding, and that the UDRP remedy will be stayed pending the outcome of the litigation). Similar protections are guaranteed under the new URS procedure. *See* URS, *supra* note 67, § 13 ("The URS Determination shall not preclude any other remedies available to the appellant, such as UDRP (if appellant is the Complainant), or other remedies as may be available in a court of competent jurisdiction.").

137. *See Rules for Uniform Domain Name Dispute Resolution Policy*, *supra* note 135

> A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding,

participating in the trusted notifier program, UDRP adjudicators are never expected to give complainants the benefit of the doubt when deciding the merits of a complaint.[138] Whether they do or not in practice is subject to debate, but there is certainly no pro-complainant bias written into the UDRP, as there is written into the trusted notifier program.[139]

V. Understanding the Stakes and Consequences

This section pulls back from the legal and operational mechanics of the trusted notifier program to consider what notice and takedown in the DNS means for right holders, domain name registrants, Internet users, and the future of the DNS. I explain why right holders want content regulation through the DNS; why registrants and Internet users are wise to resist it; and how ICANN, by facilitating the MPAA program, has compromised its institutional mission to protect the technical integrity and content neutrality of the DNS.

A. A Cheap and Efficient Process for Right Holders

From the perspective of right holders, the DNS is a much more efficient field for copyright enforcement than courts are. Thorny questions of sovereignty, jurisdiction, and choice of law can be avoided when DNS intermediaries agree to privately adjudicate and remedy claims of online infringement.[140] Litigation over

---

> new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

138. *Id.*

139. *Id.*

140. The problems associated with public adjudication of cross-border intellectual property disputes are illustrated clearly in the Canadian case of *Equustek Solutions Inc. v. Jack*, a trademark and trade secrets case in which the trial court ordered Google, a nonparty, to delist all of the defendants' second-level domains from search results on a global basis (*i.e.,* in *all* TLDs). *See* Equustek Sols. Inc. v. Jack, [2014] 374 D.L.R. (4th) 537 (B.C.S.C.). The Supreme Court of Canada upheld the global injunction. *See* Google Inc. v. Equustek Sols. Inc.,

"pirate sites" is expensive. Defendants are often located outside the United States and decline to submit to the jurisdiction of U.S. courts. Plaintiffs in such cases can (and do) seek injunctions against nonparty intermediaries, including DNS intermediaries, requiring them to cut off services to non-cooperative defendants.[141] Such injunctions, however, are subject to due process challenge, because the enjoined intermediaries are strangers to the litigation and operate at arm's length from the adjudicated infringers.[142]

If copyrights are privately enforced in the DNS through a notice-and-takedown protocol, accused operators of "pirate sites" can be brought to heel entirely outside the machinery of public courts. All it takes is a simple notice from a complaining right holder and a quick edit to a database—the zone file for the TLD in which the domain name for the offending site is registered. From a purely technical standpoint, once due process barriers are removed and a DNS intermediary agrees to cooperate, blocking public access to a website by preventing the site's domain name from resolving to the registrant's chosen Internet Protocol (IP) address is trivially easy.

[2017] 279 A.C.W.S. (3d) 822 (Can.). Google challenged the order in U.S. court, arguing that the Canadian court lacked jurisdiction to order delisting on a global basis, and that the order violates both the First Amendment and principles of international comity. *See* Google Inc. v. Equustek Sols. Inc., et al., No.-5:17-cv-04207 (N.D. Cal. July 24, 2017).

141. *See, e.g.*, Elsevier Inc. v. www.Sci-Hub.org, No. 15 CIV. 4282 RWS, 2015 WL 6657363, at *6 (S.D.N.Y. Oct. 30, 2015) (ordering nonparty "TLD Registries for the Defendants' websites, or their administrators, [to] place the [Defendant's] domain names on registryHold/serverHold as well as serverUpdate, serverDelete, and serverTransfer prohibited statuses, until further Order of the Court"); *see also* ABS-CBN Int'l v. FreePinoyChannel.com, No. 15-61002-CIV-DIMITROULEAS/SNOW, 2015 WL 11023803, at *1 (S.D. Fla. July 28, 2015) (purporting to bind domain name registrars); Preliminary Injunction at 1, Arista Records, LLC v. Tkach, No. 1:15-CV-03701-AJN (S.D.N.Y. June 1, 2015), ECF No. 53 (purporting to bind "domain name registrars, domain name registries, and Internet service providers.").

142. *See* Annemarie Bridy, *Three Notice Failures in Copyright Law*, 96 B.U. L. REV. 777, 818–29 (2016) (arguing that such orders are in most cases impermissible under Rule 65 of the Federal Rules of Civil Procedure because courts issue them with no hearing or fact-finding on the question of "active concert or participation" by the enjoined nonparty).

B. A Problematic Process for Registrants and Users

From the perspective of registrants and website users, however, privately administered blocking of entire Internet domains raises serious issues relating to transparency, fair process, and freedom of expression. The threat of accidental over-blocking looms large considering past experiences with DNS blocking of child pornography and sexually explicit content deemed harmful to minors.[143] In 2011, when the FBI seized MOOO.COM, 84,000 subdomains were shut down in an effort to seize just ten.[144] In an earlier effort to target websites distributing material "harmful to minors," ISPs implementing legislatively mandated domain blocking took hundreds of thousands of innocent sites offline to eliminate a handful that were actually distributing material prohibited by the statute.[145]

These incidents of massive over-blocking show that the potential for collateral damage to lawful speech is substantial where the targets of enforcement are not individual files or URLs but entire second-level domains. That potential is even more acute in cases involving copyrights than it is in cases involving child pornography, because infringing content online is harder to confidently identify on cursory inspection.[146]

---

143. *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 610 (E.D. Pa. 2004) (discussing an example of blocking sexually explicit content deemed harmful to minors); *see also* Matt Liebowitz & Paul Wagenseil, *Oops! Child-Porn Seizure Shuts Down 84,000 Innocent Sites*, NBC NEWS (Mar. 30, 2011), http://www.nbcnews.com/id/41649634/ns/technology_and_science-security/t/oops-child-porn-seizure-shuts-down-innocent-sites/#.V79A3zV76Hx (last visited Oct. 12, 2017) (discussing an example of blocking child pornography) (on file with the Washington and Lee Law Review).

144. *See* Liebowitz & Wagenseil, *supra* note 143 (describing the results of the MOOO.COM subdomain seizures).

145. *See Ctr. for Democracy & Tech.*, 337 F. Supp. 2d at 651

> Verizon blocked hundreds of thousands of web sites unrelated to . . . targeted child pornography when it used DNS filtering to block access to a sub-page of the Terra.es web site, a large online community[website]. . . . One [blocked website] was for a Spanish geological survey, and defendant acknowledged that [it] did not contain child pornography.

146. *See, e.g.*, Capitol Records, LLC v. Vimeo, LLC, 826 F.3d 78, 96–97 (2d Cir. 2016) (explaining why it is difficult for an ordinary person to ascertain whether a sound recording posted to the Internet—even a popular or highly

Over-blocking has also been an issue in copyright enforcement, with recent research showing high variability in the quality and accuracy of right holder takedown demands under the Digital Millennium Copyright Act (DMCA).[147] Even sophisticated right holders acting in good faith make flagrant mistakes with takedown notices.[148] For example, Warner Bros. studios recently demanded in a single notice that Google remove links in search results to Warner's own website, authorized video streaming services including Amazon and Sky, and the popular film information service IMDB.[149] Some DMCA notifiers given "trusted" status by ISPs have engaged in takedown practices that strongly suggest intentional abuse.[150] Google reported in a recent submission to the U.S. Copyright Office that 99.95% of all "infringing" links identified in notices from right holders participating in the firm's Trusted Copyright Removal Program (TCRP) were entirely fabricated.[151] Such a statistic counsels

---

recognizable recording—is copyright infringement).

147. *See* Jennifer M. Urban et al., *Notice and Takedown in Everyday Practice* 28 (UC Berkeley Pub. Law Research Paper No. 2755628, 2016), http://ssrn.com/abstract=2755628 (concluding, based on thousands of observations, that notice and takedown's effectiveness is highly dependent on who is using it and how it is practiced).

148. *See, e.g.*, *Warner Brothers Reports Own Site as Illegal*, BBC (Sept. 5, 2016), http://www.bbc.com/news/technology-37275603 (last visited Oct. 12, 2017) (noting a flagrant takedown notice mistake involving Warner Brothers and Google) (on file with the Washington and Lee Law Review).

149. *See id.* ("Film studio Warner Brothers has asked Google to remove its own website from search results, saying it violates copyright laws.").

150. *See* Section 512 Study: Request for Additional Comments, Comments of Google to the U.S. Copyright Office (Feb. 21, 2017), https://www.scribd.com/document/340085542/Google-Additional-Comments-USCO-Section-512-Study# (last visited Oct. 12, 2017) (highlighting widespread abuse in takedown practices) (on file with the Washington and Lee Law Review).

151. *Id.* at 7. Google's search algorithm considers the number of DMCA notices received for specific sites and down-ranks sites for which a high number of notices are received. *See* GOOGLE, HOW GOOGLE FIGHTS PIRACY 40–41 (2016), https://drive.google.com/file/d/0BwxyRPFduTN2TmpGajJ6TnRLaDA/view (showing how this design gives notifiers an incentive to vastly overstate the amount of infringement occurring on sites they would like to see dramatically down-ranked).

healthy skepticism about the wisdom of trust-based takedown regimes.[152]

The technical ease with which DNS enforcement can be accomplished further raises the risk of over-enforcement. Error costs are low for intermediaries, because they are generally insulated from liability to their customers through disclaimers in their terms of service.[153] By contrast, a business with a wrongfully blocked domain name may suffer irreparable harm, particularly if it has no way to appeal an open-ended suspension or an outright cancellation. Considering the magnitude of the over-blocking risk, technical precision, fair process, and competent, neutral adjudication are extremely important where domain name suspensions and cancellations are employed to police website content.[154]

There is some question, too, about the efficacy of site blocking by DNS intermediaries when determined infringers are involved.[155] While preventing a domain name from resolving to its corresponding IP address deters the vast majority of users from reaching a particular website, DNS blocking does not actually remove any allegedly infringing content from the Internet.[156]

---

152. *See* GOOGLE, *supra* note 151, at 40 (describing how Google gives trusted status in the TCRP to 114 unnamed right holder "partners").

153. *See, e.g.*, *GoDaddy Domain Name Registration Agreement*, GODADDY, https://www.godaddy.com/agreements/showdoc.aspx?pageid=REG_SA (last updated July 11, 2017) (last visited Oct. 12, 2017) (giving the domain name registrar broad authority to "cancel the registration of a domain name . . . if that name is being used, as determined by GoDaddy in its sole discretion, in association with spam or morally objectionable activities," including but not limited to "[a]ctivities prohibited by the laws of the United States and/or foreign territories in which you conduct business") (on file with the Washington and Lee Law Review).

154. *Id.*

155. *See, e.g.*, *UK Site Blocking Gives Boost to Pirate Linking Sites*, TORRENTFREAK (Jan. 2, 2015), https://torrentfreak.com/uk-site-blocking-gives-boost-to-pirate-linking-sites-150102/ (last visited Oct. 12, 2017) (discussing the use of VPNs and proxies as a way of circumventing ISP-imposed domain blocking) (on file with the Washington and Lee Law Review).

156. *See* CDT, THE PERILS OF USING THE DOMAIN NAME SYSTEM TO ADDRESS UNLAWFUL INTERNET CONTENT 2–3 (2011), https://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf (characterizing DNS web content policing as ineffective, with overbreadth impacting technology, compromising cybersecurity, and creating disputes).

Anyone who knows the IP address for a website whose domain name is blocked can (in many common server configurations) access the site directly by entering its IP address, in lieu of the domain name, into a browser address bar.[157] Ordinary users may not know that they can circumvent DNS blocks in this way, but moderately sophisticated users—a group to which steadfast "pirates" usually belong—are wise to this workaround.[158]

C. A Process Outside ICANN's Authority and Competence

For those who understand both ICANN's limited remit and the operation of the DNS, drawing a bright line between trademark and copyright enforcement through the DNS is easy enough to do. Although trademarks and copyrights are both forms of intellectual property, policing trademarks *in* domain names and policing copyrights in content *underlying* domain names are demonstrably different propositions. The use of trademarks in domain names at least arguably implicates an addressing function that could concern ICANN: The ability of an Internet user to reach the website for a brand of goods or services when she enters a domain name containing that brand's word mark into the address bar of her web browser. For example, a user looking for Pandora Internet Radio might expect to find it at Pandora.com. If the user were to find instead the website for Pandora jewelry or iHeartRadio, her resulting confusion—potentially actionable under trademark law—could conceivably be characterized as an addressing problem.[159]

---

157. *See id.* at 2 (explaining the workaround).

158. *See id.* (theorizing that "[s]avvy users could . . . [avoid] any DNS servers that have been ordered to block").

159. Glynn Lunney and Jennifer Rothman have both argued that courts over the years have went overboard in protecting trademarks in domain names, particularly with respect to so-called initial interest confusion, which is seldom material to a consumer's ultimate purchasing decision. *See* Glynn S. Lunney, Jr., *Trademarks and the Internet: The United States' Experience*, 97 TRADEMARK REP. 931, 935 (2007) (discussing the origin of the "radically overbroad Internet form" of the initial interest confusion doctrine); Jennifer E. Rothman, *Initial Interest Confusion: Standing at the Crossroads of Trademark Law*, 27 CARDOZO L. REV. 105, 108 (2005) (arguing that the doctrine of initial interest confusion violates both the Lanham Act and the First Amendment).

Online copyright infringement is different.[160] It surely creates problems and causes actionable harms for copyright holders, but those problems and harms are external to the navigational operation of the DNS.[161] Michael Froomkin made exactly this point in 2011, with respect to then-circulating proposals that ICANN expand its regulatory portfolio beyond cybersquatting to reach other claims, including copyright infringement:

> These suggestions have all differed from the UDRP in one critical fashion: whatever its merits or evils, the UDRP is designed to combat an ill—cybersquatting—that is a direct result of the structure of the DNS. In contrast, all of the other proposals that have bubbled up from time to time involve harms that are not direct results of the DNS; they may be torts or crimes that result from use of the Internet, but they are not specific to the DNS, and so far ICANN, to its credit, has shown no appetite for taking them on.[162]

Time has shown that Froomkin was right to qualify his optimism about ICANN's restraint. The foregoing discussion of ICANN's facilitating role in the MPAA–Donuts/MPAA−Radix trusted notifier program demonstrates that ICANN has at least some appetite for using the DNS as a means of regulating online

---

Recent case law, however, suggests that those excesses are being corrected. *See, e.g.*, Toyota Motor Sales, U.S.A., Inc. v. Tabari, 610 F.3d 1171, 1179 (9th Cir. 2010)

> Outside the special case of trademark.com, or domains that actively claim affiliation with the trademark holder, consumers don't form any firm expectations about the sponsorship of a website until they've seen the landing page—if then. This is sensible agnosticism, not consumer confusion . . . . So long as the site as a whole does not suggest sponsorship or endorsement by the trademark holder, such momentary uncertainty does not preclude a finding of nominative fair use.

160. ICANN long ago recognized that online *trademark* infringement, writ large, is also different—when it limited the UDRP to claims of cybersquatting despite pressure from trademark holders to broaden the program's scope to include claims of trademark infringement and dilution arising from website content (e.g., offers to sell counterfeit products). *See supra* Part III (discussing the intentionally narrow scope of the UDRP). By limiting the UDRP to address-based trademark claims, ICANN in the early days steered clear of content regulation.

161. *See* Froomkin, *Almost Free*, *supra* note 19, at 215 (pointing out that copyright harms do not impact the navigational and addressing functions of the DNS).

162. *Id.*

content.[163] It would just prefer to look the other way while registry operators do it—all in the name of Public Interest Commitments. Whereas ICANN continues to repeat the mantra that it is not in the business of policing content, its contracts with new gTLD intermediaries tell a different story—one of regulatory outsourcing that disserves the interests of registrants and, ultimately, Internet users.[164]

VI. Conclusion

The MPAA's trusted notifier program is among a growing number of privately negotiated voluntary enforcement agreements between corporate copyright holders and Internet intermediaries.[165] It is the first of its kind, however, to implicate stewards of the Internet's core technical functions. That makes it different from the others in a way that should command the attention of those concerned with Internet infrastructure and governance. The subject-matter agnosticism of the published program description is also cause for alarm, suggesting that the program could expand beyond its anti-piracy origins into aone-stop shop for multidisciplinary censorship through the DNS.

No matter how vehemently ICANN officials insist that they are respecting their mission's limits, ICANN knowingly created a contractual architecture for the new gTLDs that supports an unprecedented program of private, DNS-based content regulation on behalf of copyright holders and, potentially, other "trusted"

---

163. *See supra* Parts IV.B–C (discussing ICANN's approval of the trusted notifier program as a means of regulating content).

164. *Cf.* REBECCA MACKINNON ET AL., CTR. FOR INT'L GOVERNANCE INNOVATION, CORPORATE ACCOUNTABILITY FOR A FREE AND OPEN INTERNET 1 (2016), https://www.cigionline.org/sites/default/files/documents/GCIG%20no.45.pdf (asserting that, to the detriment of human rights, "governments, companies and a range of other non-state actors are pursuing short- and medium-term interests and agendas regarding how the Internet should be used and governed with whatever legal, regulatory, financial, political and technical tools happen to be available").

165. *See generally* Annemarie Bridy, *Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 185 (John Rothchild ed., 2016) (providing an overview of the various voluntary enforcement agreements).

parties.[166] Moreover, in creating that architecture, ICANN did nothing to secure any procedural protections or uniform substantive standards for domain name registrants who find themselves subject to this new form of DNS regulation.[167] That omission should be a red flag for those who worry that ICANN's newly minted independence from the U.S. government will make its internal governance more susceptible to capture by powerful commercial and governmental interests.[168]

For now, non-judicial notice and takedown practices in the DNS are limited; however, demands on intermediaries for stronger online content regulation across the board are growing.[169] It is easy

166. For example, representatives of the pharmaceutical industry want DNS intermediaries to suspend domain names associated with illegal online pharmacies. Like the MPAA and the RIAA, they have demanded that ICANN use its contractual compliance process to require notice and takedown for sites alleged to infringe their patent and trademark rights. *See* Letter from Carmen Catizone, Exec. Dir., Nat'l Ass'n of Bds. of Pharmacy, to Allen Grogen, Chief Contractual Compliance Officer, ICANN 1 (July 30, 2015), https://www.icann.org/en/system/files/correspondence/catizone-to-grogan-30jul15-en.pdf ("NABP requests that if a domain name is alleged to be used for the illegal or unlicensed sale of prescription drugs, at a minimum, an 'appropriate response' and 'investigation' by the registrar under Section 3.18 must include requesting that the registrant produce jurisdictional license or authorization.").

167. *See supra* Part IV.D (discussing the trusted notifier program's lack of procedural safeguards).

168. The debate over the IANA transition focused almost entirely on how to prevent ICANN from becoming captured by its most assertive stakeholders and how to ensure its accountability in the absence of DOC oversight. *See, e.g.*, LENNARD G. KRUGER, CONG. RESEARCH SERV., THE FUTURE OF INTERNET GOVERNANCE: SHOULD THE UNITED STATES RELINQUISH ITS AUTHORITY OVER ICANN? 2 (2016), https://fas.org/sgp/crs/misc/R44022.pdf (stating that "the U.S. government's authority over the IANA functions has been viewed by the Internet community as a 'backstop' that serves to reassure Internet users that the U.S. government is prepared and positioned to constitute a check on ICANN under extreme circumstances," including "capture or undue influence by a single stakeholder or by outside interests").

169. Recent targets include terrorism and hate speech. *See, e.g.*, Olivia Solon, *Facebook, Twitter, Google and Microsoft Team Up to Tackle Extremist Content*, GUARDIAN (Dec. 5, 2016), https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content (last visited Oct. 12, 2017) (discussing a plan to create a shared database of 'unique digital fingerprints' that can identify images and videos promoting terrorism) (on file with the Washington and Lee Law Review); *see also* Mark Scott, *Europe Presses American Tech Companies to Tackle Hate Speech*, N.Y. TIMES (Dec. 6, 2016), http://www.nytimes.com/2016/12/06/technology/europe-hate-speech-facebook-

to imagine programs like the MPAA's expanding soon to serve a much broader universe of notifiers—including private and governmental actors targeting what they perceive as fake news, hate speech, and terrorist propaganda. Lack of transparency and due process in such programs will make them inherently vulnerable to inconsistency, mistake, and abuse and could transform the DNS into a potent tool for suppressing disfavored speech.

---

google-twitter.html?_r=0 (last visited Oct. 12, 2017) ("Amid growing security tensions in . . . the Western World, governments, intelligence agencies, and advocacy groups want Google, Microsoft and other technology companies to take further steps to curb hate speech on digital platforms, as well as to clamp down on how terrorists circulate information online.") (on file with the Washington and Lee Law Review). Right holders are also demanding notice and takedown in the DNS for legacy gTLDs in addition to new gTLDs. *See* Letter from Steven M. Marks, Gen. Counsel, RIAA, to Steve Crocker, Chairman of the Bd., ICANN, and Fadi Chehade, CEO, ICANN 1–2 (May 12, 2015), https://www.icann.org/en/system/files/correspondence/marks-to-crocker-chehade-12may15-en.pdf

> [W]e believe there should be strong protections against online copyright infringement in all TLDs, whether legacy gTLDs or new gTLDs, and that any gTLDs that particularly target music or digital content should have increased commitments to guard against such infringement. . . . We expect ICANN to ensure this happens in a responsible and effective manner.