IP JUSTICE

An international civil liberties organization that promotes Internet freedom, innovation policy, and balanced intellectual property laws.
www.ipjustice.org

IP JUSTICE JOURNAL: Internet Governance and Online Freedom Publication Series

Internet Infrastructure and IP Censorship

By David G. Post[1] ~ 1 August 2015

Many scholars and other observers of developments in Internet governance, law, and policy have commented upon an unusual and important phenomenon that has become more widespread in recent years: using control over access to critical portions of the Internet's technical infrastructure – the system comprising the underlying protocols for routing, naming, and addressing, along with related technical standards and the agreements, formal and informal, through which they are implemented across the Internet, what Laura DeNardis calls "Critical Internet Resources" (CIRs)[2] - to enforce private and public law.

Three examples illustrate the nature of this new phenomenon.

1. The UDRP In the realm of private law and the enforcement of private rights, the paradigmatic illustration is ICANN's[3] Uniform Dispute Resolution Procedure

[1] Senior Fellow, Open Technology Institute/New America Foundation. Comments welcome: david.g.post@gmail.com.

[2] Laura DeNardis, *Internet Points of Control as Global Governance*, available at https://www.cigionline.org/sites/default/files/no2_3.pdf.

[3] ICANN is the Internet Corporation for Assigned Names and Numbers, the non-profit "multistakeholder" organization that oversees DNS policy-making and policy-implementation. The authoritative account of ICANN's formation remains Milton Mueller, *Ruling the Root* (2002). *See also* David G. Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace,* chap. 10 ("Names") (2009) and sources therein.

(UDRP).[4] The UDRP is an ICANN-operated mandatory arbitration process that deals with "cyber-squatting," *i.e.*, the practice of registering domain names that mirror (or closely resemble) existing trademarks, for the purpose of re-selling the domain name to the trademark owner. The UDRP allows a trademark holder to submit a cyber-squatting complaint to an ICANN-accredited arbitrator, who is charged with applying ICANN's substantive rules[5] for determining whether the cyber-squatting offense has been committed.

Decisions by the UDRP arbitrators are enforced *solely* through control over a particular CIR - the Internet's domain name system ("DNS").[6] That is, UDRP arbitrators can't award monetary damages of any kind, nor can they impose any punishment or other liability on the offending cyber-squatters themselves; instead, if they rule in the trademark owner's favor, they are authorized only to either (a) cancel the offending domain name registration, *i.e.*, to remove it from the set of interlocking databases constituting the DNS, or (b) transfer the registration from the defendant to the trademark holder, *i.e.*, to substitute the trademark holder for the defendant in those database entries.

[4] The UDRP was adopted in August, 1999, shortly after ICANN was formed. *See UDRP Timeline,* available at https://www.icann.org/resources/pages/schedule-2012-02-25-en. On the URDP, *see* https://www.icann.org/resources/pages/help/dndr/udrp-en.

[5] The substantive UDRP Rules require the trademark holder to show that the challenged domain name (a) is "identical or confusingly similar" to its trademark, and that the person who registered the domain name (b) "has no legitimate rights" to it and (c) acted "in bad faith." Evidence of "bad faith" includes circumstances indicating that the name was acquired "primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the . . . owner of the trademark or to a competitor of that complainant . . ." *See Uniform Dispute Resolution Policy,* available at https://www.icann.org/resources/pages/policy-2012-02-25-en.

[6] On the DNS generally, *see* Post and Kehl, *Controlling Internet Infrastructure, Part 1,* at 3-8, available at http://www.newamerica.org/oti/controlling-internet-infrastructure/, or http://tinyurl.com/q8eoyy4; National Research Council, *The Internet's Coming of Age* (2001); David G. Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace,* chap. 10 (2009); National Academy of Sciences, *Signposts in Cyberspace: The Domain Name System and Internet Navigation* (2005), available at https://www.cs.cornell.edu/people/egs/beehive/narc-dns.pdf.

The arbitrator accomplishes this by ordering the domain name *registrar*[7] that issued the offending registration to delete (or modify, in the case of a transfer) the database entry corresponding to that domain name, and to communicate that deletion/modification to the relevant domain name *registry*. Enforcement of the arbitrator's order is assured by the contracts under which ICANN enforces its policies across the DNS:[8] *Registrars* must promise, as a condition of obtaining and maintaining ICANN's accreditation, to enforce all UDRP orders;[9] *registries,* in turn, must promise, as a condition of obtaining and maintaining *their* accreditation with ICANN, to only do business with ICANN-accredited registrars, and to process all UDRP-imposed changes communicated to them by registrars; and, finally, registrars promise to issue domain names only to *registrants* who agree, in *their* contracts with registrars, to be bound by UDRP decisions.

Thus, although ICANN itself has no formal regulatory or law-making authority, its UDRP rules and procedures apply globally, binding *all* domain name registrants, registrars, and registries in *all* TLDs under ICANN's control,[10] wherever they may be located, to comply with ICANN-promulgated cyber-squatting rules.

It's a tightly woven enforcement web, and over the 15 years or so of its existence, the UDRP has proven to be a remarkably powerful global conflict-resolution system; as

[7] A "registrar" is an entity that sells (or otherwise distributes) access to individual domain names to members of the public ("registrants"). GoDaddy, Network Solutions, Register.com, and Tucows are among the better-known domain name registrars. A "registry" is an entity that manages and controls the authoritative database ("zone file") containing the names and IP addresses within each top-level domain ("TLD" - *e.g.,* .com, .org, .biz, .uk, etc.). Registries do not interact directly with the public, but receive registration information, which they implement in the TLD zone file, from the registrars.

[8] Chapter 4 ("The ICANN-based Contractual Web") of Lee Bygrave's *Internet Governance by Contract* (2015) contains an outstanding analysis of ICANN's contractual undertakings and the contractual basis for its powers. *See also Controlling Internet Infrastructure*, *supra* note 6. at 21-24.

[9] *See* Section 3.8 of ICANN's Registrar Accreditation Agreement (obligating registrar to comply with UDRP), available at https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa.

[10] It should be noted that ICANN does not exercise contractual control over the *entire* DNS; most of the country-code TLDs ("ccTLDs" – *e.g.,* .uk, .br, .jp, etc.) do not have direct contractual relationships with ICANN, and are not obligated to enforce UDRP judgments or impose a requirement on registrants that they comply with the UDRP rules (though some have done so voluntarily). See *Controlling Internet Infrastructure, supra* note 6, at Box 3.

of 2013, over 50,000 cases, from 175 countries, had been disposed of quickly and efficiently[11] (though whether they have done so fairly is very much open to dispute[12]). It derives a great deal of its power from its ability to solve three of the most challenging problems surrounding law enforcement on a largely borderless medium like the Internet: (1) the problem of choice of law (*i.e.*, determining *whose* substantive rules apply to conflicts involving persons located in different countries), (2) the problem of judgment enforcement (*i.e.*, obtaining enforcement of a legal judgment issued in one jurisdiction against a wrongdoer located in a different jurisdiction), and (3) the problem of scale (*i.e.*, functioning effectively across a medium that is, as James Grimmelmann nicely put it, "sublimely large,"[13] and one that continues to expand in size at an exponential rate). Under the UDRP, one set of rules – ICANN's – applies to all disputes, eliminating the choice of law problem. They can be effective entirely without reference to the physical location of *any* of the parties involved – the complaining trademark owner, the domain name registrant, the registrar who issued the domain name in question, or the registry of the relevant TLD – because they can be enforced through the globally-effective domain name databases themselves. And because the UDRP leverages off of existing automated mechanisms to process domain name registration information,[14] it can operate effectively at Internet scale; it is impossible to

[11] *See e.g.* Christie, *Online Dispute Resolution – The Phenomenon Of The UDRP,* in Torremans (ed), *Research Handbook on Cross-Border Enforcement of Intellectual Property* (forthcoming 2015), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2433380:

> "The system has shown it is capable of resolving cross-border IP disputes in a timely manner and at very low cost. It has delivered largely consistent outcomes across a huge volume of cases, while evolving to address scenarios that were unforeseen and unforeseeable at its implementation. It has . . . won international respect as an expedient alternative to judicial options for resolving trademark disputes arising across multiple national jurisdictions."

[12] Compare Christie's treatment of the UDRP, *id.,* with Komaitis, *The Current State of Domain Name Regulation: Domain Names as Second Class Citizens in a Mark-Dominated World* (Routledge 2012) (UDRP is "based on illegitimate grounds, its procedures are substantially flawed and unfair, it restricts the rights of domain name registrants, and it is crowded with examples of inconsistent and biased decisions"), and Geist, *Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, available at http://aix1.uottawa.ca/~geist/geistudrp.pdf).

[13] James Grimmelmann, *The Internet is a Semicommons*, 78 Fordham L. Rev. 2800, 2803 (2010).

imagine any set of national courts managing to process this volume of litigation as quickly, and at such low cost.[15]

2. SOPA/PIPA The UDRP was, in a sense, "proof of concept": control over the DNS can serve as effective leverage to enforce legal rights Internet-wide. Perhaps because "cyber-squatting" covers a relatively narrow slice of conduct, it has not received (and probably does not warrant) an enormous amount of public attention. But such was not the case for the second example of DNS-based enforcement, the ill-fated Stop Online Piracy Act (SOPA) (and its companion bill, the Protect-IP Act (PIPA) introduced in the U.S. Congress in 2011.

SOPA/PIPA targeted the activities of "foreign infringing websites," and would have authorized federal prosecutors, and private rightsholders in certain circumstances, to "seize" the domain names associated with such sites.[16] If the court agreed that the

---

[14] That is, the DNS architecture and protocols are optimized to process vast amounts of domain name registration information, and to propagate that information across the millions of Internet domain names servers, quickly and accurately. A registrar's "Cancel" or "Modify" command that is issued in response to a UDRP arbitrator's order is processed in precisely the same manner as the many hundreds of thousands of such commands circulating through the DNS on a daily basis in the ordinary course.

[15] UDRP proceedings are substantially less complex, less expensive, and less time-consuming than, *e.g.,* filing a cyber-squatting complaint under the federal Anti-Cybersquatting Protection Act in U.S. federal court. *See* Kilpatrick, ICANN Dispute Resolution Vs. Anticybersquatting Consumer Protection Act Remedies, 2002 Hous. Bus & Law Rev., available at http://www.hbtlj.org/v02/v02_kilpatrick.pdf; World Intellectual Property Organization, FAQ: Internet Domain Names, available at http://www.wipo.int/amc/en/center/faq/domains.html (most UDRP proceedings are concluded within two months, and cost between $1500 and $2000 dollars (not including lawyers' fees, if any).

[16] *See* Lemley, Levine, & Post, "Don't Break the Internet," available at http://www.stanfordlawreview.org/online/dont-break-internet, for a detailed description and analysis of SOPA/PIPA; *see also* Zittrain, Albert, & Solow-Niederman, "A Close Look at SOPA," available at http://blogs.law.harvard.edu/futureoftheinternet/2011/12/02/reading-sopa/. Technically speaking, authorizing the domain name "seizure" was accomplished by authorizing courts to proceed *in rem* – against the domain name itself, rather than *in personam* against the operator of the website or the owner of the domain. Styling them as *in rem* meant that the court would have had jurisdiction to adjudicate the claim without hearing from (or having personal jurisdiction over) the operator of the site or the owner of the domain, which would be constitutionally impermissible in an *in personam* action.

In this context, of course, "seizure" is a legal fiction; the court wouldn't take actual "possession" of anything, it would merely have the right to order the relevant domain name registry to take certain steps with respect to the name, much in the manner of the UDRP.

site in question was a "foreign infringing site . . . dedicated to the theft of U.S. property," or had "facilitated the commission of" infringing acts, the statute authorized it to order a wide range of Internet intermediaries – ISPs, domain name registrars, and domain name registries, along with a variety of financial intermediaries – to take "all technically feasible and reasonable measures" to prevent end-user access to those sites, including "measures designed to prevent the domain name of the foreign infringing site (or portion thereof) from resolving to that domain name's IP address."

Many factors contributed to the astonishing and unprecedented "surge of mobilization" that greeted (and ultimately overwhelmed) SOPA and PIPA,[17] but one important component of the extraordinary public campaign against the bills was the notion that the bills threatened, in the words of one of the influential documents published at the time, to "break the Internet" through its use of court-ordered DNS filtering:[18]

> [T]he bills represent an unprecedented, legally-sanctioned assault on the Internet's critical technical infrastructure. Based upon nothing more than an application by a federal prosecutor (or, in certain circumstances, an intellectual property rights holder) alleging that a foreign website is "dedicated to infringing activities," Protect IP authorizes courts to order all U.S. Internet service providers, domain name registries, domain name registrars, and operators of domain name servers - a category that includes hundreds of thousands of small and medium-sized businesses, colleges, universities, nonprofit organizations, and the like - to take steps to prevent the offending site's domain name from resolving to the correct Internet protocol address, . . . even when the domains in question are located outside of the United States, and registered in top-level domains (e.g., .fr, .de, or .jp) whose operators are themselves located outside the United States[.]

[17] *See* Benkler *et al*., "Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA debate," available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295953, for an extraordinarily illuminating analysis of how the public campaign against SOPA/PIPA developed over time. *See also* Larry Downes, "The Revolt Against Congress' New Internet Piracy Proposals," available at http://www.forbes.com/sites/larrydownes/2011/11/28/the-revolt-against-congresss-new-internet-piracy-proposals/.

[18] "Don't Break the Internet," *supra* note 16; *see* Benkler et. al., *supra* note 17, at 33-34, for an extended analysis of the effect of this publication on the anti-SOPA/PIPA movement.

> Directing the remedial power of the courts towards the Internet's technical infrastructure in this sledgehammer fashion . . . threaten[s] the fundamental principle of interconnectivity that is at the very heart of the Internet. The Internet's Domain Name System ("DNS") is a foundational building block upon which the Internet has been built and upon which its continued functioning critically depends; it is among a handful of protocols upon which almost every other protocol, and countless Internet applications, rely to operate smoothly. Court-ordered removal or replacement of entries from the series of inter-locking databases that reside in domain name servers and domain name registries around the globe undermines the principle of domain name universality - the principle that all domain name servers, wherever they may be located across the network, will return the same answer when queried with respect to the Internet address of any specific domain name. Much of Internet communication, and many of the thousands of protocols and applications that together provide the platform for that communication, are premised on this principle.[19]

The defeat of SOPA/PIPA has not, however, stopped US law enforcement efforts to fight alleged overseas intellectual property infringement using the DNS as the primary enforcement tool. Prof. Annemarie Bridy has comprehensively documented the Department of Homeland Security's use of the civil forfeiture provisions of federal law to "seize" thousands of domain names in recent years on the grounds that they "facilitated the production or distribution of infringing content," accomplished by ordering the relevant domain name registries to redirect web traffic from the "seized" domains to a site displaying an anti-piracy banner bearing the logos of Homeland Security Investigations, the IPR Center, and the DOJ. [20]

3. ICANN and the "Public Interest"

Compelling domain name registries and registrars to enforce arbitrator awards (Illustration 1) or court orders (Illustration 2) as a way to police access to the DNS is not

[19] "Don't Break the Internet," *supra* note 16. A number of other influential documents from within the technical community also made the argument that SOPA/PIPA threatened the security and stability of Internet's underlying technical infrastructure. *See* Internet Society, "Perspectives on Domain Name System (DNS) Filtering," available at http://www.isoc.org/internet/issues/dns-filtering.shtml; Crocker et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," available at http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

[20] Annemarie Bridy, "Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy," 46 Ariz. St. L. Rev. 683 (2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378633; *see also* Karen Kopel, "Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice," available at http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1994&context=btlj

the only way in which this portion of core Internet infrastructure can be utilized for private and public law enforcement purposes. A third example – somewhat more complicated than the first two, but no less troubling – illustrates yet another route via which infrastructure control can be used for private and public rights enforcement.

In 2013, as part of its program of opening up the top-level domain space to hundreds of new top-level domains (like .app, .blog, .pharmacy, .attorney, .brussels, .property, . . . joining the more familiar .com, .edu, .org domains) ICANN inserted two new provisions into the "Registry Agreement" that it requires operators of top-level domain registries to sign.[21] One provision ("Specification 7")[22] requires registry operators to "implement and adhere to" a set of "mandatory rights protection mechanisms (RPMs)" described in ICANN's "Trademark Clearinghouse."[23] This is a "flow-through" requirement; that is, registries must include a similar provision in their contracts with all registrars with whom they do business, obligating the *registrars* to implement the RPMs, and registrars must include a similar provision in *their* contracts with end-users (domain name registrants).

A second provision ("Specification 11") requires registries to comply with various "Public Interest Commitments" (PICs), one of which requires registries to deal with (i.e., accept domain name registrations from) *only* those registrars who:

> (a) include, in *their* contracts with domain name registrants, a provision "prohibiting registrants from distributing malware, abusively operating botnets, phishing, *piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law";*

[21] *See* Post, "ICANN, Copyright, and the 'Public Internet,'" available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/03/09/icann-copyright-infringement-and-the-public-interest/; Controlling Internet Infrastructure, *supra* note 16, at Box 5 ("ICANN as Global Law Enforcer").

[22] *See* Specification 7, ICANN Base Registry Agreement, available at https://www.icann.org/resources/pages/registries/registries-agreements-en.

[23] *See* http://www.icann.org/en/resources/registries/tmch-requirements

(b) "take reasonable and prompt steps to investigate" any reports that registrants are engaging in any such activity "contrary to applicable law"; and

(c) "respond appropriately" to such reports, "providing consequences for such activities *including suspension of the domain name."*[24]

Additionally, all participants in this contractual web – registries, registrars, and registrants – must promise to "adhere to any remedies ICANN imposes"[25] should they not live up to these PICs, including termination of their ICANN accreditation (and an immediate end to their business operations).

Notably, these two provisions were not developed under ICANN's "consensus policy development process,"[26] but were introduced at the behest of specific constituencies: the IP rightsholders (Spec. 7), and the Government Advisory Committee (Spec 11).[27]

One does not have to have too fertile an imagination to see how these provisions could enlist registrars and registries in an ICANN-directed process to enforce a broad range of laws – "*piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or [any] activity contrary to applicable law"* - via the DNS database entries. If ICANN were to choose to enforce these contractual promises, registries and registrars would risk losing their accreditation (and therefore their ability to continue their DNS-related business activities in any fashion) if they did not satisfy *ICANN* that they are taking "appropriate steps" to suspend end-users who engage in "piracy" or any activity "contrary to applicable law. Registries and registrars would need to develop policies and procedures for investigating charges of unlawful activity, and for

[24] *See* Specification 11, ICANN Base Registry Agreement, available at https://www.icann.org/resources/pages/registries/registries-agreements-en.

[25] ICANN has set up a new dispute resolution process - the "PICDRP" – to enforce registries' obligations under Specification 11. *See* https://www.icann.org/resources/pages/picdrp-2014-01-09-en.

[26] ICANN's "Consensus Policy Development Process" is described in Annex A to the ICANN Bylaws, available at https://www.icann.org/resources/pages/governance/bylaws-en.

[27] *See* GNSO gTLD Registries Stakeholder Group Statement, available at https://forum.icann.org/lists/comments-base-agreement-05feb13/pdfdrhgnqELY3.pdf.

suspending domain name registrations based on a determination that unlawful activity had taken place - subject to satisfying *ICANN* that their efforts are "reasonable" and "appropriate." Is it reasonable and appropriate – *in ICANN's view* – to revoke a domain name upon receipt of a letter from local law enforcement officials? Or a letter from the RIAA? Does the registrar have to notify the domain name registrant before taking action? Hold a hearing to provide the operator of the domain name an opportunity to defend him/herself? Examine the sites to see if they are indeed acting "contrary to applicable law"? Consult its lawyers about which law is "applicable" to the sites in question, and whether the conduct in question violates it?

ICANN has strenuously disavowed any intention of enforcing these contract terms in this way:

> "ICANN cannot be put in the position of requiring suspension of domain names on the basis of allegations of blasphemy, hate speech, holocaust denial, political organizing, full or partial nudity or a host of other content that may be illegal somewhere in the world. That would be inconsistent with ICANN's mission, ICANN's limited remit, and ICANN's responsibility to operate in accordance with a consensus-driven multistakeholder model."[28]

But what was the purpose of inserting these provisions into the contracts if there were no intention of enforcing them? Why has ICANN set up a new dispute resolution process to hear claims that registries/registrars are not complying with these promises – the PICDRP, see note 25 – if it does not intend to invoke that process? How will ICANN manage to fend off the pressure from these (or other) constituencies to require more active registrar/registry cooperation in these enforcement tasks?[29]

What are We to Make of These Developments?

The examples above, though they differ from one another in a number of important ways, share one critical feature: they each describe a *governance* scheme – the

[28] Alan Grogan (ICANN Chief Compliance Officer), "ICANN is not the Internet Content police," available at https://www.icann.org/news/blog/icann-is-not-the-internet-content-police.

[29] *See* Post, supra note 21, for a description of efforts by the Motion Picture Association of America and the Recording Industry Association of America in this direction.

imposition of binding rules upon vast numbers of Internet users – exercised by means of control over the DNS databases and over access/entry thereto.

One does not have to be Tiresias the Seer to predict that we will be seeing a great deal more of this kind of thing – or at least a great deal more pressure, from private rightsholders and public authorities alike, to introduce and implement this kind of thing - in the future.[30] These infrastructure-based systems are efficient in ways that the ordinary conventional mechanisms of international law cannot hope to match: fully automated judgment execution mechanisms that can operate, virtually instantaneously, on anyone in any corner of the planet. They solve – or, more precisely, they serve as a work-around - the seemingly intractable problems of conventional international law – choice of law, judgment execution, and scale – that have made applying private or public law across the Internet so difficult. It is entirely predictable – indeed, virtually inevitable - that they will be pressed into service under many new guises and in many new implementations in the years to come.

How should we be thinking about this development? Perhaps governance-by-infrastructure is a new, innovative alternative to the cumbersome traditional approach of relying on local law and local courts, one that can help to bring the Rule of Law to the Internet, protecting legal rights and enforce legal norms on a medium where such protection and enforcement have been difficult to come by? Why *not* use the DNS, or other components of core Internet infrastructure, to catch the bad guys and throw them off the Internet?

There are, I believe, many reasons why that is a bad idea. Though an exhaustive compendium of all of the troubling features of government-by-infrastructure regimes is beyond the scope of this paper, there is a set of *core concerns* that implementation of such regimes inevitably raise, which can be organized into five categories: concerns

[30] *See* Milton Mueller, *Ruling the Root* (2002) at 219 (discussing the "use and exploitation of data generated by Internet identifiers to facilitate surveillance and control of Internet users by law enforcement agencies," and concluding that "if the ICANN regime survives, this aspect of policymaking will probably play a much larger role in the future [inasmuch as] the use of a centralized identification mechanism that gives authorities both the ability to identify private actors and some control over their access to cyberspace will probably prove to be too tempting to pass up").

about Internet neutrality, legitimacy and institutional competence, due process, free expression, and harm to third parties.

Internet Neutrality

As has been extensively discussed in recent years - most notably, in connection with the "net neutrality" debate - the basic Internet design incorporates a powerful neutrality/non-discrimination principle, generally known as the principle of "end-to-end design."

> The Internet is unusual among networks in putting most of the intelligence in the computers at the edge of the network, rather than in the infrastructure at the heart of the network. The network forwards packets with only minor processing—all the heavy lifting takes place on the transmitting and receiving computers. This approach of putting intelligence at the edge of the network is known as the end-to-end principle, and it is one of the keys to the Internet's success thus far.[31]

Smart machines connected to a dumb network; complicated and sophisticated applications running over a network that does little more than moving bits around as

---

[31] Felten, "The Nuts and Bolts of Net Neutrality," available at https://www.cs.princeton.edu/courses/archive/fall09/cos109/neutrality.pdf. *See also* Clark and Blumenthal, "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," available at http://nms.lcs.mit.edu/6829-papers/bravenewworld.pdf:

> "End to end arguments suggest that specific application-level functions usually cannot, and preferably should not, be built into the lower levels of the system—the core of the network. Even if parts of an application-level function can potentially be implemented in the core of the network, the end to end arguments state that one should resist this approach if possible."

Lemley and Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era," 48 UCLA L. Rev 925 (2001) ("The end-to-end argument counsels that the 'intelligence' in a network should be located at the top of a layered system - at its 'ends,' where users put information and applications onto the network. The communications protocols themselves (the 'pipes' through which information flows) should be as simple and as general as possible"); Wu, "Application-Centered Internet Analysis," 85 Va. L. Rev 1163 (1999) ("end-to-end holds that, wherever possible, function should not be placed at the lower-levels of a network system - rather, everything possible should be left to the applications at the 'ends.' In other words, the lower-level protocols should focus only on the minimal function of transmitting data, and in all other respects be kept as simple, unintrusive, and open as possible"); Post, *supra* note 3:

> "In an end-to-end network, the Network does the minimum number of tasks required to get messages from one place to another. Network Layer protocols are stripped down to their essentials; they do only what is necessary to get bit-strings where they are supposed to go. All other functions are left for the senders and the recipients, the network end-points . . . As long as messages are formatted in accordance with the Network Layer addressing rules, the Network protocols will get them to the right place; what happens next is none of its concern . . . Smart machines, connected to a dumb network. Complicated and sophisticated applications, and a network doing nothing more than moving bits around as directed by those applications. That's the Internet. All the interesting stuff is at the edges the network just gets the bits there, as quickly and efficiently as possible."

directed by those applications. End-to-end design counsels that core Internet infrastructure protocols should focus to the maximum feasible extent on performing only that minimal bit-transport function, while staying as simple, unintrusive, and open as possible in all other respects.

Adherence to the end-to-end design principle has, without question, contributed mightily to both the Internet's astonishing growth, and to the explosion of innovation and creativity that it has stimulated across the globe.[32] It is not, to be sure, some kind of sacred or inviolable principle; even its most fervent adherents recognize that, as the Internet continues to evolve, there may be cause for deviating from the strict end-to-end model.[33] But we should do so with great care and exercising great caution, lest we interfere with a critical source of the Internet's power, and thereby kill the goose that is laying the golden egg.

The inter-locking protocols and databases that constitute the Internet's DNS are optimized to perform one role as part of the network's core message-transport function: resolving names into IP Addresses, quickly and reliably. All the processing required to "discriminate" among messages – based upon their content, or the identity of the sender or recipient – is kept *out* of the core.

---

[32] Lessig and Lemley, *supra* note 31:

> "The effect of [end-to-end design] has been profound. By its design, the Internet has enabled an extraordinary creativity precisely because it has pushed creativity to the ends of the network. Rather than relying upon the creativity of a small group of innovators working for companies that control the network, the end-to-end design enables anyone with an Internet connection to design and implement a better way to use the Internet. Because it does not discriminate in favor of certain uses of the network and against others, the Internet has provided a competitive environment in which innovators know that their inventions will be used if useful. By keeping the cost of innovation low, it has encouraged an extraordinary amount of innovation in many different contexts. By keeping the network simple, and its interaction general, the Internet has facilitated the design of applications that could not originally have been envisioned."

See also Wu, *supra* note 31 (describing end-to-end's "deeper effects" as "giving application writers the freedom to innovate whenever and however they like [while] confining the network itself to simple functions of broad usage,' thereby allowing "future applications unknown or unpredictable at the time of design.. . . And at least in part as a result of these features, this decade has witnessed an astonishing development both of Internet applications existing at the beginnings of the Internet (like email) and totally new and extremely innovative applications. All of this might have been impossible, or at least difficult, if the Internet had not had an end-to-end design.").

[33] *See* Clark and Blumenthal, *supra* note 31.

Governance-by-infrastructure upsets that careful delineation of function.[34] The DNS now has additional roles to play (requiring additional processing) – helping to control copyright infringement, or phishing, or consumer fraud, or the distribution of child pornography, or human trafficking, or any number of other possibly worthwhile goals – that reach far beyond the one task it is required to perform (*viz.*, accurate name/address resolution). The DNS is no longer neutral, but an instrument for discriminating against certain kinds of content and certain users. The unforeseen and possibly unforeseeable consequences of re-purposing Internet infrastructure in a manner contravening the fundamental e2e principles that have guided the development of that infrastructure up to now are likely to be severe.[35]

Legitimacy

Governance-by-infrastructure raises profound – and profoundly troubling – questions of legitimacy, authority, and institutional competence. Whether or not one believes that access to the Internet is a fundamental human right, the power to control access to the global communications platform is a formidable one, and it should only be exercised by those duly authorized to do so. To put the question bluntly: What gives ICANN - or whomever is in control of DNS policy implementation - the right to tell a Bangladeshi domain name registrar, or a Brazilian domain name registrant, or a South Korean domain name registry, that their respective businesses are no longer operable because they have been eliminated from the DNS databases? That ICANN is not authorized to make global policy regarding the appropriate steps necessary for the identification and elimination of copyright infringement, or consumer fraud, or child pornography, or the like is apparent from a glance at its structure and organization; though it is indeed a "multi-stakeholder" institution, its community of stakeholders represents – intentionally - a very narrow slice of the larger Internet community, focused overwhelmingly on individuals and entities involved in specialized technical tasks (IP addressing, naming, and numbering). This is hardly the structure one would

[34] *See* note 19.

[35] *See id*.

come up with when designing an institution to tackle, on an Internet-wide basis, any of those very difficult and politically contentious tasks.

Due Process

Efficiency of judgment entry and execution in governance-by-infrastructure regimes is a double-edged sword. There may well be, at this moment, hundreds of thousands, or more likely millions, of domain names associated with Internet sites hosting infringing content; the costs, in time and money, of providing each of them with anything resembling due process – adequate notice, and a reasonable opportunity to be heard before a neutral – so that a fair determination can be made as to whether they are acting unlawfully or not, are prodigious.

Those costs, however, must be borne, somewhere in the system – at least, if we believe in the principle of due process and the rule of law. But of course the core Internet infrastructure is almost entirely in private hands, and private entities may not feel themselves bound to respect user due process rights – especially when it is so costly to do so.

Freedom of Expression

Domain names warrant special protection because, as Annemarie Bridy puts it, they are "dual-use" properties, enabling both lawful and unlawful activity and serving not only as "gateways to vast repositories of digital property but also (and relatedly) as instrumentalities of speech."[36] A single domain name allegedly tainted by unlawful activity "may provide access to a mix of unlawful and lawful content, [and] telling the difference between the two can be challenging for judges even after the benefit of full discovery. "Seizure" of allegedly offending domain names is thus "the twenty-first century equivalent of padlocking the bookstore." Anyone who believes in the paramount value of uninhibited free expression should be especially suspicious of mechanisms that too-easily (and too-efficiently) take these speech instrumentalities out of the hands of individuals.

[36] Bridy, *supra* note 20.

Third-party Harm

The hierarchical nature of the Internet's DNS virtually assures that the elimination, via "seizure" or cancellation, of individual domains will affect large numbers of innocent third parties. Each level of the domain name hierarchy can encompass a virtually unlimited number of subdomains – *i.e.*, each top-level domain can include many millions of 2d-level domains, each of which can include many millions of 3d-level domains, each of which can include many millions of 4th-level domains, and so on, down 127 levels.[37] Many online services rely on this feature to assign individual subdomains – davidgpost.wordpress.com - to users as a means of allowing them to post their own content.[38] Blocking the resolution of a domain at any level (because of unlawful content or activity taking place at a site utilizing that domain) necessarily means that *all* lower-level subdomains are blocked as well – even if they are completed independent of the offending site and are pursuing entirely lawful activities.

> Perhaps the most egregious example of collateral damage resulting from a domain seizure occurred . . . in February 2011, when ICE seized the "mooo.com" domain for allegedly pointing to illegal content. The seizure resulted in over 84,000 subdomains of mooo.com being blocked. Mooo.com is a service that allows users to register subdomains, which they can then point to Internet content hosted at any IP address. No content is hosted immediately under the mooo.com domain; all content — including personal blogs, discussion forums, small business sites, and sites where academic researchers share papers and professional information — is hosted under subdomains that take the form "username.mooo.com." The content hosted under any particular subdomain is wholly distinct from the content hosted under other subdomains. *But because of illegal content allegedly present at one such subdomain, all were blocked when the "parent domain," mooo.com, was seized*.

[37] *See Controlling Internet Infrastructure*, *supra* note 6, at 3-9 (describing how each of the millions of 2d-level domains within the .edu top-level domain (*e.g.*, StateU.edu) can support a vast number of 3d-level domains (*e.g.*, Compsci.StateU.edu), each of which can support a vast number of 4th-level domains (Admin.Compsci.Stateu.edu), and so on).

[38] Familiar examples include blogspot.com, wordpress.com, wix.com, squarespace.com, and rojadirecta.com, each of which operates a "hosting service" by assigning a subdomain (*e.g.,* [username].blogspot.com]) to individual users. Hosting services operating in this manner, in the aggregate, account for millions of individual websites.

This kind of "collateral damage" by over-blocking is a persistent, and may well be an inevitable, feature of governance-by-infrastructure schemes.[39] At the very least, it calls for the most assiduous attention to due process protections so as to minimize, to the extent possible, the damage such schemes can wreak on expression and communication by innocent third parties.

Conclusion

Governance-by-infrastructure is here to stay, likely to be a part of the global legal landscape far into the future. It is too efficient, and too powerful, for it to be otherwise, and it needs to be deployed with the greatest of care, for it raises deep questions of fairness, transparency, and due process. The Internet has thrived as a neutral and open communications platform, and its continued vibrancy depends on our ability to maintain that neutrality and openness to the maximum extent possible in the months and years to come.

[39] *See* sources cited in note 20. *See also* "Brief of Amici Curiae Electronic Frontier Foundation, Center For Democracy and Technology, and Public Knowledge in Support of Puerto 80's Petition For Release Of Seized Property," available at https://www.eff.org/files/filenode/puerto80_v_US/2011-06-20-rojadirecta.pdf (detailing "overblocking" by DHS "seizure" operations, including a single "seizure" that eliminated over 80,000 non-infringing websites); *CDT v. Pappert*, 337 F. Supp. 2d 606 (E.D. PA. 2004) (in an effort to comply with blocking orders relating to fewer than 400 child pornography websites, more than a million completely unrelated and innocent websites were blocked).