THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVIII STLR.ORG SPRING 2017

ARTICLE

GOVERNING INTERNET TERRITORY: ICANN, SOVEREIGNTY CLAIMS, PROPERTY RIGHTS AND COUNTRY CODE TOP-LEVEL DOMAINS†

Milton L. Mueller* and Farzaneh Badiei**

This paper examines the legal and Internet governance controversies over country code top-level domain names (ccTLDs). In recent litigation (*Weinstein v. Islamic Republic of Iran and ICANN*), terrorism victims argued that ccTLDs are property and attempted to seize Iran's .IR domain for compensation. In refusing to uphold this claim, an appeals court ruled that a court-ordered redelegation would impair the Internet Corporation for Assigned Names and Numbers' (ICANN's) role in global Internet governance. While the .IR case is recent, the underlying tensions between state sovereignty, the role of ICANN and the rights of organizations that have been awarded ccTLDs have been simmering for two decades. Three governance models are in play: a sovereignty-based model, a property rights/market-based model, and a global public trustee model. The legal and political science literature leaves this Internet governance issue unexplored and unsettled, while court rulings on the property status of domains have been mixed or indecisive. Most legal scholars merely *assume* that states have sovereignty rights over their ccTLDs and do not critically assess the justification for, or the implications of, a sovereignty-based model. Likewise, many legal scholars, governments and Internet governance institutions have resisted recognizing TLD delegations as a property right, but

* Milton L. Mueller is a professor at Georgia Institute of Technology School of Public Policy.

** Frazaneh Badiei is a research associate at Georgia Institute of Technology School of Public Policy, and the Executive Director of Internet Governance Project (IGP).

their arguments are often based on misunderstandings of the economics and technology of the domain name system. Drawing on law, economics and sovereignty theories, this paper shows that top-level domain names have all the essential features of a property right. It argues that a governance regime that recognized them as such would be preferable to a regime based on sovereignty claims or a global public trustee model.

1. INTRODUCTION

Political geographer Philip Steinberg has noted the "historical, ongoing and, at times, imaginary projection of social power onto spaces whose geophysical and geographic characteristics make

them resistant to state territorialization."[1] Political power gets projected, in varying ways, onto the oceans, outer space, and the Arctic. The Internet is no exception to this tendency—despite the fact that nations and territories are not recognized in the Internet protocols. Internet Protocol addresses, unlike telephone numbering conventions, are not structured by territory or jurisdiction but are global.[2] Internet routing protocols recognize network operators, not nations. The Domain Name System (DNS) provides a global standard for assigning unique character strings that function as Internet addresses anywhere in the world.

But some top-level domain names *refer* to countries—in other words, there is a semantic linkage between political territory and domain name resources. Nearly 200 top-level domains are based on an international standard (ISO-3166) that assigns two-letter alphabetic codes to internationally recognized geographical territories (e.g., .BR for Brazil or .IN for India).[3] These domains have come to be known as country code top-level domains

---

1. Philip E. Steinberg, *Profile Page of Professor Philip E. Steinberg*, DURHAM UNIV., https://www.dur.ac.uk/research/directory/staff/?mode=staff&id=11830 (last visited March 17, 2017). The de-territorialized, global nature of social communities in cyberspace has long been asserted by various scholars. For example, they claim that communication via electronic means create new and alternative spaces to conventional territories for social and cultural interaction and formation of communities. CAROLYN SHAFFER & KRISTIN ANUNDSEN, CREATING COMMUNITY ANYWHERE: FINDING SUPPORT AND CONNECTION IN A FRAGMENTED WORLD (1993); Shelagh J. Squire, *Re-Territorializing Knowledge(s): Electronic Spaces and Virtual Geographies*, 28 AREA 101, 102 (1996). This does not mean that territorialization does not happen in cyberspace. As Goldsmith and Wu argue, such globalization on the Internet is indeed affected by territorial governmental coercion. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 184 (2006).

2. The Internet Assigned Numbers Authority (IANA) is responsible for global coordination of the Internet Protocol addressing systems. The policies for allocation of IP addresses are set by the Internet Corporation for Assigned Names and Numbers (ICANN). The allocation of IP addresses is not based on the decisions of the states or territories but based on policies set by ICANN and Regional Internet Address Registries. *Global Addressing Policies*, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, https://www.icann.org/resources/pages/global-addressing-2012-02-25-en (last visited March 17, 2017).

3. *Country Codes - ISO 3166*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/country_codes (last visited Aug. 8, 2016). To view a list of ccTLDs, refer to IANA Root zone Database. *Root Zone Database*, INTERNET ASSIGNED NUMBERS AUTHORITY, http://www.iana.org/domains/root/db (last visited Aug. 8, 2016).

("ccTLDs"). Country code TLDs function in exactly the same way as more familiar top-level domains such as .COM or .ORG. But their association with geographic territories sets up an interesting interaction between the Internet's global virtual space, traditional concepts of political territory, and various standards for asserting rights to control territory. By "standards for asserting rights" we refer specifically to property rights claims and sovereignty claims. Can the right to control a ccTLD be considered a property right, owned by a private party and tradable in a market? Or is control of a ccTLD an extension of the state's sovereign rights? Or does a third model apply—that of a public trustee administered by the Internet Corporation for Assigned Names and Numbers ("ICANN"), the global organization that coordinates the root of the domain name system ("DNS")?[4] ICANN is a private nonprofit corporation organized under California law.[5] Because of its technical coordination role in the domain name system, ICANN must be involved in the award of a top-level domain name to a specific party.[6] Unless ICANN enters the appropriate technical

4. The domain name system is a name space based on a hierarchical structure. The root, which is administered by ICANN, is the beginning of the hierarchy. ICANN delegates top-level domains (TLDs such as .COM, .UK, .EDU or .TV) to registries, and the top-level domain registries sub-delegate second-level domains (such as GATECH.EDU) under their top-level domain. Some TLD registries have only generic categories at the second-level (such as .AC, .CO, or .GOV) and assign users third-level domain names (e.g., BANK.CO.UK).

5. Article 3 of the Articles of Incorporation of Internet Corporation for Assigned Names and Numbers stipulates that ICANN "is a nonprofit public benefit corporation organized under the California Nonprofit Public Benefit Corporation Law for charitable and public purposes. The Corporation is organized and operated exclusively for charitable, educational, and scientific purposes within the meaning of § 501(c)(3) of the Internal Revenue Code of 1986, as amended (the "Code"), or the corresponding provision of any future United States tax code." *Amended and Restated Articles of Incorporation of Internet Corporation for Assigned Names And Numbers*, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, https://www.icann.org/resources/pages/governance/articles-en. https://www.icann.org/resources/pages/governance/articles-en (last updated 3 October 2016).

6. "The process of ccTLD delegation or redelegation is initiated when a formal request is submitted to the Root Zone Management staff at ICANN. The request and all required documentation is then reviewed and verified by these ICANN staff members. After the review and authorisations are completed, the request is implemented as a change to the Root Zone and Root Zone Database. Upon successful completion of the process, the new country-code domain is established, or a transfer takes place in the case of redelegation of an existing ccTLD." *Delegating or Redelegating a Country-code Top-level Domain*

data into the DNS root zone, the delegee does not have control over the management of or registration within the domain.

This paper explores the legal and economic rationales for conceptualizing ccTLDs as property rights, sovereign rights, or public trusts administered by ICANN. It explores the consequences of each approach and asks which model provides for the most efficient and equitable form of governance. The problem posed involves an unusual and interesting interaction of international relations, public international law, private law and technical protocols. By engaging with these questions, the paper attempts to provide useful insights into the nature of sovereignty in cyberspace, and practical insights into the best way to handle conflicting claims over ccTLD delegations.

This is not a purely theoretical issue. In recent litigation involving the top-level domain for Iran (.IR), plaintiffs sought to seize control of a country code domain in order to compensate victims of terrorist acts allegedly backed by the Iranian state. The plaintiffs characterized the ccTLD as a form of property that could be confiscated under civil law. Similar cases seeking to attach ccTLDs have affected Syria (.SY), North Korea (.KP)[7] and the Congo (.CG).[8] The Congo case was based on a commercial dispute and not on terrorism claims.

A view of ccTLDs as property subject to attachment or 'garnishment' has been reinforced by the fact that the global authority for domain names is not an intergovernmental treaty organization organized around principles of sovereignty, but ICANN. Because it is a U.S. private sector corporation, ICANN's role seemingly subjects ccTLD delegees to civil law claims of the sort seen in the Iran and Congo cases.

On the other hand, using American courts to settle claims over country domains strikes many as incongruous. In fact, governments have been keen to assert sovereignty rights over the ccTLDs referring to their country. States began to intervene in the ICANN environment after 1999 to claim exclusive authority over

---

(ccTLD), INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/help/cctld-delegation (last visited Aug. 8, 2016).

7. Rubin, et al. v. Islamic Republic of Iran, et al., 270 F.R.D. 7 (2010); Nonparty ICANN's Opposition to Plaintiff's Motion to Compel Production of Documents in Response to Subpoena, Haim, et al. v. Islamic Republic of Iran, et al., 425 F. Supp. 2d 56 (D.D.C Mar. 2006) (No. 02-1811-RCL); Stern, et al. v. Islamic Republic of Iran, et al., 73 F.Supp.3d 46 (D.D.C. 2014).

8. C. Itoh Middle East EC v. Internet Corporation for Assigned Names and Numbers, No. SC090220 (Cal. App. Dept. Super. LA Nov. 14 2006).

delegation and public policy for ccTLDs.[9] Sovereignty claims are especially important to countries that have geopolitical conflicts with the U.S. (such as Iran, Russia and China); the claims are thought to immunize them from external claims of authority or control.[10] Complicating the picture both politically and legally, ICANN has held its status as the authoritative manager of the DNS by virtue of a contract with a single sovereign: the United States of America.[11] This contractual tether to a single state sets up an internal contradiction within the putatively private sector-based, sovereignty-free governance regime of ICANN.

While property is a private right and sovereignty is a public right,[12] international relations theorists have argued that they have some commonalities.[13] Both, for example, involve claims of exclusive control.[14] Both are also invoked in allocating rights over other international resources, such as the sea and outer space.[15]

In the theory and practice of Internet governance, there is a tendency to resist recognizing domain name delegations as a property right.[16] Most litigation around domain name property

---

9. See *infra* section 3b.

10. Islamic Republic of Iran, *Contribution from the Islamic Republic of Iran to the Global Multistakeholder Meeting for the Future of the Internet, 23-24 April 2014 Sao Paolo, Brazil*, NETMUNDIAL http://content.netmundial.br/contribution/contribution-from-the-islamic-republic-of-iran-to-the-global-multiskaeholder-meeting-for-the-future-of-the-internet-23-24-april-2014-sao-paolo-brazil/236 (last updated April 2014).

11. Note that the United States has ended its special "stewardship" role and fully privatized it. *IANA Functions Contract*, NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION, https://www.ntia.doc.gov/page/iana-functions-purchase-order (last visited March 17, 2017).

12. Morris Cohen stated: "The distinction between property and sovereignty is generally identified with the Roman discrimination between dominium, the rule over things by the individual, and imperium, the rule over all individuals by the prince. Morris Cohen, *Property and Sovereignty*,13 CORNELL. L. REV. 8 (1927).

13. *See generally* John Gerard Ruggie, *Continuity and Transformation in the World Polity: Toward A Neorealist Synthesis*, 35 WORLD POLITICS 261 (1983).

14. Ruggie explains that "The chief characteristic of the modern concept of private property is the right to exclude others from the possession of an object. And the chief characteristic of modern authority is its totalization, the integration into one public realm of parcelized and private authority." *Id.* at 275.

15. *See* Eric Husby, *Sovereignty and Property Rights in Outer Space*, 3 J. INT'L L. & PRAC 359 (1994).

16. Indeed, some resist recognizing any property rights in cyberspace, *e.g.* Anupam Chander, *The New, New Property*, 81 TEXAS L. REV. 715 (2003). Some other scholars believe that digital information might be in fact some sort of

rights has occurred over registrations at the second level of the domain name hierarchy, but some cases also pose this issue for top-level domains. Opponents of property claims argue either that domain name delegations are trustee relationships and/or that they are contracts for service, not a form of property.[17] Those advancing the trustee arguments oppose property rights because it is feared that property claims would disrupt the prevailing model of Internet governance.[18] The courts have been divided on the question of domain names' status as property. Some court cases have found that second-level domains are not property, but services. Other decisions have upheld their status as a property right.[19]

What, then, is the best way to shape the relationship between existing or prospective ccTLD delegees, ICANN, and the government of the territory referenced by a ccTLD string? What role should sovereignty or property rights claims play? The scholarly literature has left these questions unsettled, even unexamined. There are some descriptive papers and books about the relationship between states and the ccTLD delegee,[20] as well as studies of the relationship between states and ICANN.[21] Studies that consider the triangular relationship among ICANN, ccTLD delegees and states are rare, and those that exist have not applied property rights and sovereignty theories. Insofar as it deals with

---

property. Hardy said, "A limitation on what others may do with digital information might well take the form of some sort of property right." Trotter Hardy, *Property (and Copyright) in Cyberspace*, U. CHI. LEGAL F. 217, 218 (1996). Radin also argues that how we think about property might change in the age of new technology and the digital economy but she argues that the old idea of property is reinstated on cyberspace. Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J.L. & COM. 509 (1995). Some also believe in limited property rights. Rose argues that in cyberspace we need to develop limited common property rights. Carol Rose, *Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129, 132 (1998).

17. Motion to Quash Writ of Attachment, Haim v. Islamic Republic of Iran, 425 F. Supp. 2d 56 (D.D.C. Mar. 24, 2006) [No. 14-7193].

18. *See* Weinstein v. Islamic Republic of Iran, 831 F.3d 470 (D.C. Cir. 2016).

19. *See infra* Section 5c.

20. *See* Y J PARK, THE POLITICAL ECONOMY OF COUNTRY CODE TOP-LEVEL DOMAINS (ProQuest 2008); Michael Geist, *Governments and Country-Code Top-level Domains: A Global Survey–Version 2.0*, 23 (University of Ottawa, Working Paper 2004); ERICA SCHLESINGER WASS, ADDRESSING THE WORLD: NATIONAL IDENTITY AND INTERNET COUNTRY CODE DOMAIN (Rowman & Littlefield, 2003).

21. GOLDSMITH & WU, *supra* note 1 at 123–126; MILTON MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 55-106 (2010).

sovereignty, most literature merely *assumes* that states have sovereignty rights over their ccTLDs, and does not directly deal with the applicability of the theories of sovereignty and property rights to this relationship.[22]

This paper uses a law and economics framework to analyze the relationship between ccTLD delegation, sovereignty rights and private property rights. Section 2 provides some basic definitions and background. Section 3 traces the historical evolution of policy regarding ccTLD delegation and redelegation rights in the ICANN process. Section 4 then reviews basic definitions and concepts of sovereignty, and critically examines the basis for governments' sovereignty claims to ccTLDs in that light. Section 5 applies economic theories of property rights to domain names and analyzes the legal precedents and legal arguments made in cases contesting domain names' status as a property right. Section 6 provides a conceptual framework for assessing the different approaches to sovereignty and property rights on global Internet governance. The paper concludes that while governments can claim sovereign control over the operation of any business in their territory, their claims to sovereignty over ccTLD delegations *per se* at the global level are unjustified. The paper also shows that domain names do have all the economic features of a property right, and argues that treating them as such would have beneficial effects on global trade in information services.

2. TECHNICAL AND INSTITUTIONAL BACKGROUND

ICANN is currently responsible for global coordination of the root of the Internet Domain Name System (DNS). The DNS refers to both a name space from which unique names can be assigned to users, and a protocol for matching these names to specific Internet protocol addresses in response to queries from Internet users' computers.[23] The DNS is a hierarchical name space, and ICANN

22. Various papers have looked into ccTLDs and states' assertion of sovereignty. These papers are focused on policy discussion and do not discuss theories of sovereignty or justifications for the claim that ccTLDs are sovereign territory. *See generally*, Kim G Von Arx & Gregory R Hagen, *Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control*, 9 RICH. J. L. & TECH. 4 (2002); Peter Yu, *The Origins of CCTLD Policymaking*, 12 CARDOZO J. INT'L & COMP. L. 387 (2004).

23. For a more extensive explanation of DNS targeted at a non-technical, non-expert audience, *see* DANIEL KARRENBERG, INTERNET SOCIETY BRIEFING PAPER, THE INTERNET DOMAIN NAME SYSTEM EXPLAINED FOR NON-EXPERTS, http://www.internetsociety.org/sites/default/files/The%20Internet%20Domain%20Na

only coordinates the top-level of the hierarchy. Its job, in less technical terms, is to ensure that each top-level domain name (for example, .UK) is globally unique and has a distinct manager with known and published contact details. For each top-level name assignment, ICANN must enter technical data into the root zone file that ensures that queries from global internet users seeking to communicate with the .UK domain are directed only to the name servers operated by the recognized .UK ccTLD manager. The existence of a mutually agreed-upon, single, authoritative root zone file is critical to the functioning of the Internet. A single, global, coordinated root zone is one of the most secure ways of ensuring that all networks and applications that use domain names—such as websites, email, or streaming media services—can be connected to all other domains regardless of jurisdiction, domain registrar, or Internet service provider.

The assignment of a top-level domain to a specific operator is called *delegation*; the party that receives the delegation is called a *delegee*. Redelegation is the process of changing the delegee, in other words, moving the delegation from one party to another. For generic top-level domains such as .COM or .ORG, the delegation process involves a contractual relationship between two parties: ICANN and the delegee. For ccTLDs, however, the delegation process is less institutionalized and less hierarchical and is built mostly on consensual relationships between ICANN, the delegee, and governments.

A. Origins of ccTLDs

The DNS protocol was first implemented around 1982. In the initial phases of its implementation, the Internet's designers defined a small set of 'generic' categories, such as .COM, .EDU, .ORG and .GOV, to serve as top-level domains (hereafter known as generic top-level domains or gTLDs). After networking researchers in Great Britain made a request for a .UK top-level domain, the Internet's developers made a fateful decision to incorporate country names into the DNS's top-level naming conventions.[24] In

---

me%20System%20Explained%20for%20Non-Experts%20(ENGLISH).pdf (last visited Apr. 4, 2017). *See generally* Peter Yu, *supra* note 22.

24. Milton L Mueller, *The Battle Over Internet Domain Names: Global or National TLDs*?, 22 TELECOMM. POL'Y 89, 92–93 (1998). *See also* A. Michael Froomkin, *Almost Free: An Analysis of ICANN's 'Affirmation of Commitments'*, 9 J. TELECOMM. & HIGH TECH. L. 187, 190–198 (2011) (describing the history of ICANN prior to 2007); JOHN KLENSIN, IETF REQUEST

order to relieve themselves of some of the risks and burdens of deciding who or what qualified as a country, they found an existing international standard (ISO-3166-1) that assigned two-letter alphabetic codes to recognized geographical territories. From 1984 on, this standard was used as the basis for creating top-level domains that corresponded to territories and countries. These became known as ccTLDs.

The ISO-3166 list was intended to provide the early Internet pioneers with a rule-based, non-discretionary and thus non-political way of responding to the demand for country-name top-level domains. For the most part, this worked. But the match between political territory, the domains the early technical pioneers assigned and the ISO-3166 list was never perfect, and this eventually allowed politics to seep in.[25] For example, the ISO-3166-1 code for Great Britain was actually GB, not UK, yet .UK became established as the ccTLD simply because that is what the early requesters asked for. A decade later, when the demand for new top-level domains became even more intense because of their money-making potential, certain politically influential entities were able to demand, and receive, two-letter top-level domains that were not on the primary ISO-3166 list but only on the reserved list.[26]

It is important to note that the ISO-3166 lists were not exactly lists of sovereign political territories. They were focused on distinct geographical areas associated with economies and included island territories politically related to larger sovereign states but not geographically conjoined to them, such as Wallis and Futuna (.WF), Isle of Man (.IM), Northern Mariana Islands (.MP), or Guernsey (.GG). Taiwan and Hong Kong, which are distinct politico-economic entities whose sovereignty was either disputed or transitional, also had their own country codes, .TW and .HK.

In the early evolution of the Internet, the island territory ccTLDs provided an avenue for entrepreneurial individuals to get the delegations and run them as a business, sometimes with the active support of the people or government in the referenced territory, but sometimes with little or no relationship to the local territory. The country code for the Indian Ocean territory (.IO) is an example of the latter case. It belongs to a British firm, the

---

FOR COMMENT 3071, REFLECTIONS ON THE DNS, RFC 1591, AND CATEGORIES OF DOMAINS (2001), https://tools.ietf.org/html/rfc3071.

25. Klensin, *supra* note 24, at 6–8.

26. The most notable example is the European Union, which used its influence with ICANN and the U.S. government to be assigned EU as a ccTLD.

Internet Computer Bureau, which obtained the delegation from Jon Postel in 1997.[27]

B. ccTLDs as Valuable Assets

Collectively, there were over 134 million second-level domains registered under ccTLDs in early 2015.[28] Registrations under ccTLDs constitute about one third of the multi-billion dollar annual market for domain name registrations. For each registration, the ccTLD registry operator usually collects a yearly fee. Thus, the operation of a ccTLD registry can be a respectably-sized business, and possession of a ccTLD delegation a valuable asset. The annual revenue of Nominet, the operator of the .UK ccTLD, was £28 million (about $42 million) in 2014.[29] DENIC, the ccTLD for Germany, pulled in €14.5 million the same year. The .IO registry charges £60/year for a second-level name,[30] generating a nearly $10 million revenue stream for its proprietor. The individual domains under a ccTLD, such as hsbc.co.uk, are worth billions more in value as identifiers of websites or services associated with Internet-based commerce and expression.

C. ccTLDs vs. gTLDs

Though many ccTLD operators are keen to differentiate themselves from their (usually) more commercial 'generic' top-level domain (gTLD) counterparts such as .COM, .NET or .INFO, in fact, there is no technical, functional or economic difference between the two. The technical function provided by .UK or .BR is exactly the same as the technical function provided by .COM or any other TLD. The DNS protocol makes no distinction between them. Moreover, consumers of domains often treat ccTLD

---

27. The delegation record of .IO is available online. *Delegation Record for .IO*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/domains/root/db/io.html (last visited Mar. 4, 2017).

28. Total country-code TLD (ccTLD) registrations were 134 million domain names, a 1.5 percent increase quarter over quarter, and an 8.7 percent increase year over year. *The Domain Name Industry Brief*, 12 VERISIGN DOMAIN REPORT 1, at 4 (March 2015), https://www.verisign.com/assets/domain-name-report-march2015.pdf.

29. *Strategic Report*, NOMINET ANNUAL REPORTS AND ACCOUNTS IN 2014, http://www.nominet.uk/wp-content/uploads/2015/08/nominet_report_and_accounts_2014.pdf (last visited March 29, 2017).

30. The price list for the .IO ccTLD is available online. *Retail Price List*, NIC.IO, https://www.nic.io/pricelist.xzx (last visited Mar. 4, 2017).

registrations and generic TLD registrations as economic substitutes. When, for example, the Chinese government imposed harsher restrictions on registrations within .CN, the number of .COM registrations in China increased its market share, as Chinese consumers shifted away from .CN registrations to registrations in .COM.[31]

Some ccTLDs have made themselves into 'quasi-generics' by exploiting similarities between their country code and other meanings. Tuvalu's .TV domain, for example, has value as a video domain and the right to run it was leased by the country to a commercial registry. Whether the ccTLD is run as a private sector nonprofit (.DE, .UK), as a government enterprise (.CN, .KR), or outsourced and run in an overtly commercial manner (.TV, .ME), however, ccTLDs and gTLDs are in the same business. The only differences are the legal and political distinctions in the way they are delegated and regulated; and these differences, as we shall see, are rooted in the semantics of the name. Registries that are gTLDs are heavily regulated by ICANN contracts, subject to ICANN policy making processes, and pay fees to ICANN. CcTLDs, on the other hand, do not (for the most part) have contracts with ICANN and make only voluntary contributions to the support of the Internet Assigned Numbers Authority ("IANA") functions.

3. ICANN AND THE DELEGATION OF CCTLDS

This section traces the historical evolution of country code top-level domain (ccTLD) delegation policy. This narrative sets the stage for the more theoretical discussions of sovereignty and property rights in the following sections, so that the reader can better appreciate the complex institutional, economic and technical environment in which the concepts will be applied.

The delegation of country code TLDs went through three phases. In the first phase, decisions were made by the developers of Internet standards and protocols, notably Jon Postel, the computer scientist at the University of Southern California Information Sciences Institute who ran the IANA. In the second phase (1998-2014), ICANN was created and tried to step into the role of Postel, but its authority over ccTLD delegations and regulation was challenged both by governments and by existing

31. CHINA INTERNET NETWORK INFO. CTR., STATISTICAL REPORT ON INTERNET DEVELOPMENT IN CHINA, https://cnnic.com.cn/IDR/ReportDownloads/201507/P020150720486421654597.pdf (Jan. 2015).

ccTLD delegees. By 2015, however, the three parties (ICANN, governments, and ccTLD operators) seemed to have reached an equilibrium around a "framework of interpretation," ushering in the third phase. This has occurred as the U.S. moved to end its unilateral authority over the DNS root.

A. Phase 1: RFC 1591

RFC 1591 is the first document that attempts to articulate a policy to govern TLD delegations.[32] It was written in 1994 in response to the need for more formal policy guidance due to the widespread adoption of the Internet protocols and growing number of requests for delegations based on the ISO-3166 standard. It is important to note that Postel's document was meant to apply to *both* ccTLDs and gTLDs.

RFC 1591 articulates neither a private property model nor a sovereignty model of TLD delegation, but rather a *global public trustee* model. In Postel's own words: "These designated authorities [TLD delegees] are trustees for the delegated domain, and have a duty to serve the community. The designated manager is the trustee of the top-level domain for both the nation, in the case of a country code, and the global Internet community."[33]

A notable feature of RFC 1591 is that the ccTLD delegee is considered a trustee not just of the nation, but of "the global internet community" as well. In other words, the relevant "public" or "community" in this model is not exclusively national. This deviates significantly from a sovereignty-based delegation model.

In any public trustee model, the delegee does not have a simple property right, but a conditional license to hold and operate a resource based on meeting some kind of standard of service to the parties for whom the resource is held in trust. Implicit in such a model is the existence of a higher-level authority, and/or some kind of procedure, to determine whether a particular trustee is meeting the needs of the relevant community. In RFC 1591 that authority was, tacitly, the IANA (i.e., Postel himself).

U.S. broadcast licenses provide another example of a public trustee licensing regime. Broadcast licenses were awarded to U.S. private companies based on a public trustee model starting in the

32. JON POSTEL, IETF REQUEST FOR COMMENT 1591: DOMAIN SYSTEM STRUCTURE AND DELEGATION (1994), https://www.ietf.org/rfc/rfc1591.txt.

33. *Id.* at 3.

late 1920s.[34] The channels were not owned by the private broadcasters but given to them by the national government for a limited, renewable period. Broadcast firms were expected to meet certain public interest requirements in order to retain their license(s). The role of selecting the appropriate trustee rested with the Federal Communications Commission—a national level regulator—even though broadcasters were meant to serve as trustees for *local* publics corresponding to the service region of the broadcaster.

Unlike U.S. broadcast regulation, RFC 1591 did not require periodic reviews and renewals of ccTLD delegees by IANA. It did, however, say that the IANA could revoke a delegation if there were "persistent problems with the proper operation of a domain" or if the "designated manager has substantially mis-behaved." Of requests to transfer the delegation from one organization to another, RFC 1591 basically assumes a non-adversarial process. It says that the IANA: "must receive communications from both the old organization and the new organization that assure the IANA that the transfer is mutually agreed, and that the new organization understands its responsibilities."[35]

The text not only ignored the possibility of conflict, but indicated that redelegation did not involve an active determination by the IANA as to which applicant would be a better trustee. IANA would merely ascertain that the local parties involved all agreed to the transfer and that the new organization understood the requirements of operating a TLD registry. However, RFC 1591 also stated that "[i]t is also very helpful for the IANA to receive communications from other parties that may be concerned or affected by the transfer."[36] This implied (weakly) that a delegee needed local support and that IANA might refuse to change the

---

34. *See* Henry Geller, *The Comparative Renewal Process in Television: Problems and Suggested Solutions*, 61 VA. L. REV. 471, 471–475 (1975) (describing the early history of the Communications Act); Marc Sophos, *The Public Interest, Convenience, or Necessity: A Dead Standard in the Era of Broadcast Deregulation*? 10 PACE L. REV. 3 663–670 (1990) (describing the development of the public interest standard); THOMAS G KRATTENMAKER & LUCAS A. POWE, JR., REGULATING BROADCAST PROGRAMMING (1994) (describing early regulation of public broadcasting). For a critique of the public trustee argument and an analysis of its shift toward a more property and market-oriented approach, *see* David Seth Zlotlow, *Broadcast License Auctions and the Demise of Public Interest Regulation*, 93 CAL. L. REV. 885 (2004).

35. POSTEL, *supra* note 32, at 6.

36. *Id.*

delegation if there was significant opposition from the local or global Internet community.

On the whole, Postel's global public trustee model for top-level domain delegation implied that the IANA, which later became part of ICANN, was the ultimate delegation authority. In this model, the state (which is not mentioned at all in RFC 1591 in connection with delegation) had no special status but is merely one of the "significantly interested parties" that "should agree that the designated manager is the appropriate party."[37]

B. Phase 2: The Contentious Period

As part of a process initiated by the U.S. government, ICANN was formed in 1998 to institutionalize the IANA and the domain name policy making process. The newly-formed ICANN viewed itself as carrying on Postel's legacy as a global governing authority based on private contracts, contracts that were supposed to encompass gTLDs and ccTLDs alike. ICANN thought it would be able to leverage its control of the DNS root to subject all TLD registries to contractual arrangements with itself.

But Postel's halo failed to rub off on ICANN. Incumbent ccTLD delegees, especially those that were independent of state authority, resisted any arrangement that would give ICANN (or the local government) the ability to expropriate or regulate them. Conversely, governments—who were now beginning to pay attention—viewed themselves and not ICANN as the appropriate governance authorities for ccTLDs. In effect, each of the three interdependent entities were seeking a form of sovereignty or exclusive authority. ICANN was asserting exclusive control of the DNS root zone and attempting to leverage that control to impose global contractual obligations upon TLD registries.[38] Some incumbent ccTLD operators considered their delegation to be a *de facto* property right that neither ICANN nor the local government

37. *Id.* at 5.

38. Many ccTLDs resisted contractual obligations with ICANN. ICANN's authority over the root zone, however, gave it enough leverage to pressure some ccTLD managers into entering contractual relationships. *See* George Christou & Seamus Simpson, *Internet Policy Implementation and the Interplay Between Global and Regional Levels*, *in* INTERNATIONAL ORGANIZATIONS AND IMPLEMENTATION: ENFORCERS, MANAGERS, AUTHORITIES? 75, 79 (Jutta Joachim, Bob Reinalda, and & Bertjan Verbeek, eds., 2004); YU, *supra* note 22, at 398–401.

could take away without the operator's consent. Governments wanted exclusive authority over delegation and public policy.[39]

Neither of the three parties, however, could unilaterally impose a solution on the others. Although they did have the power to pass legislation or executive orders to control ccTLD operators in their territory, states needed ICANN to recognize and implement their preferred ccTLD delegations in the global DNS root. While ICANN's IANA could refuse to change a root zone entry, it could not credibly threaten to eliminate established ccTLD delegees from the root zone if they failed to comply with its wishes, because that would disable service for thousands if not millions of people and undermine, if not destroy, the fledgling institution's legitimacy and support. Indeed, in those early days ICANN could have lost control of the DNS root altogether if it alienated enough registries, businesses, and governments, as they might have coalesced around an alternative DNS root.[40] CcTLD delegees needed ICANN to maintain and update their data entries in the DNS root zone, but they also could ill afford to ignore or alienate their local political authority. As a result of these conflicts, governance arrangements relied on non-binding agreements, and ccTLD delegation policy went into a contentious period that was not fully resolved for 15 years.

One of the key documents in this period was a proposed modification of RFC 1591 called ICP-1 (May 1999).[41] Written by ICANN staff and approved by its initial board without any formal policy development process, ICP-1 mirrored RFC 1591's original structure and much of its content, but modified it in ways ICANN thought reflected the new circumstances. Due to growing political pressure from governments, for example, ICP-1 added to the discussion of "significantly interested parties" the following statement: "The desires of the government of a country with regard to delegation of a ccTLD are taken very seriously. The IANA will

---

39. See the discussion of the GAC Principles later in this section and the account of the World Summit on the Information Society *infra* section 4 (b).

40. *See* Milton L. Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction?* 33 J. NETWORK INDUS. 313 (2002). *See also Alternative TLD Name Systems and Roots: Conflict, Control and Consequences*, SAC009 SSAC REPORT (2006), https://www.icann.org/en/system/files/files/alt-tlds-roots-report-31mar06-en.pdf.

41. INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS, ICP-1: INTERNET DOMAIN NAME SYSTEM STRUCTURE AND DELEGATION (CCTLD ADMINISTRATION AND DELEGATION) (1999), http://archive.icann.org/en/policies/icp-1-archived.htm.

make them a major consideration in any TLD delegation/transfer discussions."[42]

ICP-1 also contained a much more direct statement that ICANN had the authority to revoke delegations:

> (f) Revocation of TLD Delegation. In cases where there is misconduct, or violation of the policies set forth in this document and RFC 1591, or persistent, recurring problems with the proper operation of a domain, the IANA reserves the right to revoke and to redelegate a Top-level Domain to another manager.[43]

Although the same claim was made (less forcefully) in RFC 1591, governments and ccTLD managers did not trust ICANN with this authority and rejected ICP-1. CcTLDs objected to ICP-1 not only because of its substance, but because of the top-down process used in its development.

The formation of ICANN also led to the creation of a Governmental Advisory Committee ("GAC"). Although the ICANN regime for Internet governance was meant to be 'private sector-led'[44] and to keep governments at arms-length, the GAC was created in order to provide states with a role that would make the regime more acceptable to them. The GAC quickly became the venue where governments could assert their claims regarding their power over the delegation of ccTLDs. At the first GAC meeting in Berlin in May 1999, held behind closed doors, rancorous complaints about ccTLD delegations, especially delegations to island entities that were formally under some state's sovereignty, filled the air. The GAC started mobilizing the governments who were participating in ICANN around a set of principles regarding the governance of ccTLDs.

In February 2000 the GAC issued a document called *Principles for the Delegation and Administration of ccTLDs* (the "GAC Principles").[45] The GAC endorsed the concept that a ccTLD delegee was a public trustee but made the territorial sovereign the arbiter of the public trust. The GAC Principles severely curtailed

---

42. *Id.*

43. *Id.*

44. Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 10, 1998).

45. GOVERNMENTAL ADVISORY COMM., PRINCIPLES FOR DELEGATION AND ADMINISTRATION OF CCTLDS, presented by Governmental Advisory Committee (ICANN ed., 2000), https://archive.icann.org/en/committees/gac/gac-cctldprinciples-23feb00.htm.

the property rights of the delegee by asserting that the delegation "cannot be sub-contracted, sub-licensed or otherwise traded without the agreement of the relevant government or public authority and ICANN." It went further and asserted that governments should have the ultimate authority in designating the manager of the ccTLD.[46] In effect, the GAC was embracing the public trustee model, but proposing that national governments, not the IANA, should determine who the appropriate trustee would be.

Incumbent ccTLD operators were no more enthusiastic about the GAC Principles than they were about ICP-1 and contractual regulation by ICANN.[47] Nevertheless, ICANN started citing or applying the GAC Principles in many of the redelegation requests it had to handle in the mid-2000s.[48] In one incident during this period, ICANN took the delegation of the ccTLD for Australia (.AU) away from Dr. Robert Elz, a computer scientist, without his approval or consent even though no technical problems or "mis-behavior" was involved, thus violating the precepts of RFC 1591. But elbowing aside the incumbent was necessary for ICANN and the Australian government to conclude a bargain amongst themselves. Elz's replacement, the new .AU Domain Administration Corporation ("AuDA") was formally endorsed by the Australian government in December 2000, and was recognized by ICANN in October 2001. As part of the redelegation, AuDA signed one of the controversial contracts with ICANN that almost no other ccTLDs would agree to sign.[49] It also signed instruments committing itself to adhere to certain GAC Principles (at a time when the chair of the GAC was an Australian).[50] The bargain between ICANN, GAC and the Australian government presaged a division of authority that many other governments would later find

46. *Id.* § 7.4 ("With respect to future delegations or reassignment of delegations, ICANN should delegate the administration of a ccTLD only to an organisation, enterprise or individual that has been designated by the relevant government or public authority.").

47. Discussion with Martin Boyle, Senior Policy Advisor, Nominet UK, in Buenos Aires, Argentina (July 25, 2015).

48. *See, e.g.*, ccTLD Sponsorship Agreement (.au) §1.5 (2001), https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en. ("On 18 June 2001 . . . auDA reconfirmed its commitment to the Government of Australia that it will comply with clause 9 of the GAC Principles.").

49. *See id.*

50. Letter from Chris Disspain, CEO, AU Domain Administation, to Senator Richard Alston, Minister for Communications (Jun. 18, 2001), http://www.iana.org/reports/2001/au-redelegation/disspain-to-alston-18jun01.html.

acceptable: the national government would dictate to whom the domain would be delegated and the delegee would operate under government oversight, while ICANN would have authority over the global technical coordination interest.[51]

In another incident typical of this period, the .LY domain (Libya) was redelegated to the General Post and Telecommunication Company ("GPTC"), a governmental agency that operated and regulated all telecommunications services in Libya. The original delegation of the Libyan ccTLD was shrouded in confusion due to a dispute between two businessmen. The domain had been run since 1997 by an expatriate Libyan from the UK using a UK-based name server. A redelegation request in 2002 ushered in a long period of disputation over the delegation, which ICANN seemed unable or unwilling to resolve. Confused about which claimant had the authority for the domain, the company providing name service to .LY withdrew, and the entire domain became inoperative in April 2004. Under RFC 1591 or ICP-1, IANA would have had the authority to revoke and redelegate it. But the redelegation finally occurred at the behest of the Libyan government, not IANA. In requesting the redelegation, the GPTC invoked the GAC Principles. It does not appear that any stakeholder group other than the government was involved with supporting or approving the redelegation.[52] The IANA report on the .LY redelegation repeatedly refers to the GAC Principles as "best practice."[53]

In 2005, the GAC issued a revised set of principles which implicitly referred to the sovereign rights of states in the delegation and administration of the ccTLDs,[54] but included other stakeholders and the Internet community in decision-making about delegation and redelegation. Clause 7.4 was removed and replaced by clause 7.1 which reads:

> 7.1. Delegation and re-delegation is a national issue and should be resolved nationally and in accordance with

---

51. IANA REPORT, ON REQUEST OF THE .AU DOMAIN ADMINISTRATION (AUDA) FOR REDELEGATION OF .AU TOP-LEVEL DOMAIN (2001), http://www.iana.org/reports/2001/au-report-31aug01.html.

52. *See* IANA REPORT ON THE REDELEGATION OF THE .LY TOPLEVEL DOMAIN (2004), https://www.iana.org/reports/2005/ly-report-05aug2005.pdf.

53. *Id.* at 4.

54. *See* GOVERNMENTAL ADVISORY COMM., PRINCIPLES AND GUIDELINES FOR THE DELEGATION AND ADMINISTRATION OF COUNTRY CODE TOP-LEVEL DOMAINS §1.6 (2005), https://archive.icann.org/en/committees/gac/gac-cctld-principles.htm.

> national laws, *taking into account the views of all local stakeholders and the rights of the existing ccTLD Registry*. Once a final formal decision has been reached, ICANN should act promptly to initiate the process of delegation or re-delegation in line with authoritative instructions showing the basis for the decision.[55]

Despite the mentions of other stakeholders in decision-making, and despite the fact that the GAC Principles mentioned the public trustee model,[56] in practice states had the main role in delegation and redelegation. In some instances ICANN's role became purely operational. The ccTLD of Burkina Faso (.BF), for example, was initially delegated to the University of Ouagadougou in 1994, prior to establishment of ICANN. In 2008, however, Burkina Faso Law 61/AN explicitly appointed the *Autorite de Regulation des Communications Electronique* as the authority for the domain.[57] While its evaluation stated that it had sought documents describing the views of the local Internet community, it is unlikely that IANA would have given a negative evaluation of a government-backed delegee to the board, and unlikely that ICANN's board would have rejected a government-backed delegee and approved a competing delegee put forward by other stakeholders. Although it has a checklist for the requirements of delegation or redelegation, ICANN/IANA rarely gets involved with or halts a redelegation even if the resolution made between the government and the private entity is not based on equity and fairness. Some reports, however, do indicate that IANA investigates the level of community support for delegation or redelegation.[58] Whether an IANA investigation could result in a *refusal* to delegate—as opposed to just confirming a requested delegation—is another matter, however.

---

55. *Id.* § 7.1 (emphasis added).

56. *See id.* § 5.1.

57. *Approval of Redelegation of the .BF domain representing Burkina Faso* (2011), *available at* https://features.icann.org/2011-01-25-approval-redelegation-bf-domain-representing-burkina-faso.

58. In the case of .AX, the ccTLD for Aland, an island under the control of Finland, the report states that IANA sought feedback from representative groups in the community. *See* IANA REPORT ON DELEGATION OF THE .AX TOP-LEVEL DOMAIN (2006), https://www.iana.org/reports/2006/ax-report-09jun2006.pdf.

C. Phase 3: The Framework of Interpretation

As seen above, the 2014 ccTLD delegation policy was still contentious and ambiguous on key matters. Country code registries did not formally accept the GAC Principles or ICP-1 as binding policy, yet until very recently both documents were put forward by various parties as guiding policy documents.[59] In a recent court filing related to the .IR case, the U.S. government said on the one hand that ICANN is the trustee for ccTLD names and that requests of governments are not "dispositive,"[60] but on the other hand, another U.S. statement recognized nations' "sovereignty concerns" in the delegation of "their ccTLDs."[61] As the cases above show, in practice, governmental requests do seem to be dispositive. Delegation policies have evolved on a case by case basis and can be inconsistent.

Recognizing this problem, a working group on a Framework of Interpretation Working Group ("FOIWG") was created in 2014.[62] FOIWG's mission was to bring the involved parties together to develop a common interpretation of the rules and procedures for delegating and redelegating ccTLDs. The Framework of Interpretation is not intended to replace the 2005 GAC Principles. Instead, it describes and formally validates the approach worked out during the second phase, and recognizes IANA's role as merely an operational role in delegation and redelegation (i.e., implementing the delegation changes in the DNS root zone). The council of ccTLD managers in the Country Code Names Supporting Organization ("ccNSO") agreed to recommend the

---

59. For example, in the .IR litigation ICANN put forward ICP-1 as an 'authoritative policy' document, even though it is not recognized by the ccTLD managers and is not consistent with the GAC Principles. Weinstein et al vs. Islamic Republic of Iran and ICANN, 831 F.3d 470 (D.C. Cir. 2016).

60. Brief for the United States as Amicus Curiae at 14–18, *Weinstein*, 831 F.3d 470 (D.C. Cir. 2016) (No. 14-7193).

61. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. PRINCIPLES ON THE INTERNET'S DOMAIN NAME AND ADDRESSING SYSTEM (2005), http://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system.

62. FRAMEWORK OF INTERPRETATION WORKING GROUP (FOIWG), FRAMEWORK OF INTERPRETATION OF CURRENT POLICIES AND GUIDELINES PERTAINING TO THE DELEGATION AND REDELEGATION OF COUNTRY-CODE TOP-LEVEL DOMAIN NAMES (2014), https://ccnso.icann.org/workinggroups/foi-final-07oct14-en.pdf.

Framework of Interpretation proposed by the working group to the ICANN board of directors for ratification.[63]

The GAC, however, expressed doubts, as it wanted to limit the power of ICANN/IANA in delegation and redelegation so as to uphold national sovereignty. In its comments on the interim report, GAC stated that "[the report] seems to suggest that the IANA would somehow duplicate the national process, and come to a decision on the validity and weight of the views of the relevant government."[64] The GAC expressed reservations despite the fact that FOIWG enumerated the situations when the IANA can get involved with redelegation and had given it only a technical role. Recall that RFC 1591 allows the IANA to revoke a ccTLD delegation when the manager has substantially misbehaved. The FOI document interprets 'misbehavior' narrowly, in terms of technical operation. It divides misbehavior into (a) behavior that poses a threat to the stability and security of the DNS and (b) the manager's failure to perform objective requirements.[65] In the same document, it states that the IANA should not step in regarding issues of honesty, justice, equity and fairness. It does not, however, prevent the IANA operator from investigating whether the local Internet community consents to redelegation or delegation.

4. THEORIES OF SOVEREIGNTY AND CCTLDS

From the foregoing it is evident that ccTLD delegation involves a complex interaction between ICANN as root zone administrator, the territorial government, and the delegee. States want to assert sovereignty over ccTLD delegations. But on what basis do they make this claim, and what are the broader implications of recognizing such a claim? Many governments—and perhaps most people—merely assume that a ccTLD somehow belongs to a country. But what is the basis for this assumption? This question is almost never asked in discussions of ccTLDs and sovereignty, but it is essential to do so. A critical examination of this claim reveals how irrational it is, and how acting on the basis of that assumption can have many undesirable impacts on the Internet, the domain name market, and the global public interest.

---

63. CCNSO COUNCIL, FINAL REPORT FOIWG (2015), https://ccnso.icann.org/workinggroups/foi-final-resolutions-11feb15-en.pdf.

64. GOVERNMENTAL ADVISORY COMM., COMMENTS ON FOIWG INTERIM REPORT ON 'SIGNIFICANTLY INTERESTED PARTIES' (2015), https://ccnso.icann.org/workinggroups/gac-comments-foi-interim-report-sip-26sep12-en.pdf.

65. FOIWG, *supra* note 61, para. 4.5.

A. Aspects of Sovereignty

Max Weber's canonical definition of the state describes it as "that human community, which (successfully) lays claim to the *monopoly of legitimate physical violence* within a certain territory . . . ."[66] It is the combination of a supreme authority with territorial exclusivity that makes for a sovereign. Political scientist Stephen Krasner has broken down the classic concept of sovereignty into four distinct elements which, he argues, do not always coincide:[67] 1) international legal sovereignty, involving mutual recognition by other states with formal juridical independence;[68] 2) Westphalian sovereignty, involving the exclusion of external actors from the authority structures in a territory; 3) domestic sovereignty, the ability of public authorities to exercise effective control within their territory;[69] and 4) interdependence sovereignty, meaning the ability of public authorities to regulate the flow of information, ideas, goods, people, capital, etc. into and out of their borders. Contrary to the widespread perception that the Internet affects Westphalian sovereignty, the Internet's primary impact is on interdependence sovereignty in the information and communication sectors.[70]

These elements of sovereignty can be grouped into two dimensions, internal and external. Domestic sovereignty and interdependence sovereignty aspects refer to the ability of the territorial authorities to hold supreme power over a country's

---

66. MAX WEBER, *The Profession and Vocation of Politics*, *in* POLITICAL WRITINGS 309, 310–311 (Peter Lassman, & Ronald Speirs eds., 1994).

67. Stephan Krasner, *Abiding Sovereignty*, 22 INT'L POL. SCI. REV. 229, 231–233 (2001).

68. There are many subtleties here. States do not have to be *universally* recognized by other states to obtain international legal sovereignty, and sometimes there is an important distinction between the sovereign entity and a specific government (e.g., the recognition of Somalia as a sovereign entity by international actors despite the complete collapse of its government). Hence it is important to look empirically at whether states have been able to assert control over the delegation of ccTLDs by arguing that they are a recognized state. *See* Robert D. Sloane, *Changing Face of Recognition in International Law: A Case Study of Tibet*, 16 EMORY INT'L L. REV. 107, 113 (2002).

69. On the historical origins of domestic sovereignty, *see generally* DIETER GRIMM, SOVEREIGNTY: THE ORIGIN AND FUTURE OF A POLITICAL AND LEGAL CONCEPT (Belinda Cooper trans., Columbia University Press 2015).

70. *See e.g.* DAVID J. BETZ & TIM STEVENS, CYBERSPACE AND THE STATE: TOWARDS A STRATEGY FOR CYBER POWER 57–74 (2011) (applying Krasner's typology of sovereignty to cyberspace and arguing that the Internet does have its most transformative effects on interdependence of sovereignty).

internal affairs.[71] International legal sovereignty and Westphalian sovereignty pertain to *external* sovereignty, the recognition of a state by other states and its independence from foreign intervention and foreign authority structures. This section first discusses and defines the four categories of sovereignty. It will then consider their application to ccTLD delegation.

B. ccTLDs and Sovereignty

Based on these understandings of sovereignty, we now critically examine states' claim of sovereignty over the delegation of country code domain names. Recall that the Domain Name System (DNS) is a technical protocol for organizing a global name space. In computing, a namespace is defined as a set of symbols used to organize objects of various kinds, so that these objects may be referred to by an exact, unique name in software instructions. The DNS creates a hierarchical name space with an unnamed root at the top. The DNS root zone contains a list of all the top-level domain names and the IP addresses associated with them. When Internet users connect to a web site, send an email, or download a file, they are (usually) using the root zone to find out which server is associated with which top-level domain name so that they can acquire the technical data needed to communicate with the other domain.

A basic understanding of the technology makes it clear that it would be deeply problematic for the root zone of the DNS to be subject to state sovereignty. The DNS root servers respond to queries by billions of digital devices which are distributed across all of the world's sovereign territories. Because sovereignty involves supremacy and exclusivity, no single state could claim sovereignty over the contents of the DNS root zone file without generating equally justified claims from all other states. Thus, any attempt by states to extend sovereignty into the DNS root would lead to either

---

71. At first sight it might seem that interdependence sovereignty is a form of external sovereignty. However, interdependence is about domestic regulations that control the borders. Unlike external sovereignty, it does not relate to the interdependencies between states, but relates to interdependencies between a state and controlling a group. This is why, for example, Westphalian sovereignty (which is external) can exist without necessarily having interdependence sovereignty (which is internal). As Krasner argues, "A state might have little interdependence sovereignty, be unable to regulate its own borders, but its Westphalian/Vattelian sovereignty could remain intact so long as no external actor attempted to influence its domestic authority structures." Krasner, *supra* note 66, at 233.

a single preeminent state with global jurisdiction (such as the U.S.),[72] or to multiple, competing, uncoordinated name spaces that would interfere with the universal connectivity of the Internet.

The DNS root achieves global connectivity by transcending sovereignty. Similar limits on state sovereignty have been recognized and accepted from the time of Grotius. In his book *Mare Liberum* (The Free Sea), Grotius rejected British claims to sovereignty over the high seas and argued that the right of the sovereign was limited to its own territory and was not extendable.[73] The contemporary UN Convention on the Law of the Sea (UNCLOS) institutionalized this logic; while recognizing sovereign rights over territorial waters it formally defined the high seas as a sovereignty-free zone.

The argument against extending national sovereignty into the DNS root zone is largely uncontested; even the most assertive states in Internet governance have not pressed for it. Most states recognize the need for a supra-national entity to administer the DNS root zone, though they have often disagreed on whether the responsible entity should be ICANN, the ITU or something else.

Unlike the root, however, ccTLD delegations carve the DNS name space up into separately administered domains based on the ISO-3166 list. Many of the entries on that list are roughly based on what Krasner calls international legal sovereignty, i.e., mutual recognition by other states. Why, then, shouldn't the delegation of ccTLDs be subject to sovereignty claims?

We argue against recognizing a sovereignty claim for three reasons. 1) A state's lack of control over the delegation of a ccTLD registry does not undermine or defeat any of the key features of internal or external sovereignty. 2) The link between ccTLDs and

---

72. The special role of the U.S. government, which in October 1998 established the power to approve all root zone changes, requires some comment here. The initial claim of U.S. control over root zone changes was based on purely domestic concerns about the antitrust liability of the Network Solutions registry, the original government contractor maintaining the authoritative DNS root zone. Network Solution ran the root while also competing in the commercial marketplace as the operator of the .COM, .NET and .ORG domains. The U.S. never couched its role as a sovereignty claim but as "stewardship" of the DNS. Even so, the special U.S. role was never accepted by the rest of the world, and explicitly named and criticized by the World Summit on the Information Society's output (the Tunis Agenda).

73. KATHRYN MILUN, THE POLITICAL UNCOMMONS: THE CROSS-CULTURAL LOGIC OF THE GLOBAL COMMONS 87 (2011). The theory of absolute sovereignty was put forward by John Selden in *Of the Dominion, or Ownership of the Sea*. *See* JOHN SELDEN, OF THE DOMINION, OR OWNERSHIP OF THE SEA (Robbins Collection, UC Berkeley School of Law 1964) (1615).

countries is purely semantic, and a semantic reference to a country in an online name space does not automatically give the government of the country being referred to the right to control the uses and users of the name. 3) The primary impetus for sovereignty claims came from the preeminent role of one sovereign—the United States—in controlling ICANN and changes to the DNS root zone—but that preeminent role is changing, which undermines the need to assert sovereignty rights as a counterbalance to U.S. control. We elaborate on these three arguments below.

1. The Requirements of Sovereignty

A state's lack of control over the delegation of a ccTLD registry does not undermine or defeat any one of the key features of sovereignty cited in Krasner's taxonomy.

Regarding external sovereignty, it is evident that territories do not have to be recognized as sovereign under international law to be placed on the ISO-3166 list and delegated ccTLDs. As noted before, there are many ccTLDs that refer to territories not recognized as sovereign entities. The lack of correspondence between the country code list and sovereignty is especially clear from the IANA report on the delegation of the .PS ccTLD (the country code for Palestine). In deciding whether to delegate .PS, IANA stated that: "it is well-settled under current delegation policy that issues about the legal status of a listed entry on the ISO 3166 list are not pertinent to whether a ccTLD should be established and delegated."[74]

In other words, the presence of a territory on the ISO-3166 list is not the equivalent of international legal recognition.

Westphalian sovereignty, too, is not undermined or contradicted by an inability of the state to dictate to whom a ccTLD referring to it is delegated. A domain name registry using the name of a country is not necessarily an 'authority structure' within that country (though it could be made into one). A state that wants to create a state-run domain name registry that serves distinctive state purposes is not required to use the ccTLD for that;

---

74. *See* IANA REPORT ON REQUEST FOR DELEGATION OF THE .PS TOP-LEVEL DOMAIN (2000), https://www.iana.org/reports/2000/ps-report-22mar00.html ("Because the IANA is not in the business of assessing whether or not particular areas are 'countries,' the policy set forth in ICP-1 and RFC 1591 for delegation matters has been to avoid political considerations and simply refer to the ISO 3166-1 list as an independent source of two-letter abbreviations for countries and areas.").

it could apply for or acquire another TLD. It might not need a TLD at all to create authoritative domains and websites suited to its purposes; it could create them under a commercial operator's TLD. Several major states, such as Great Britain, the Netherlands and Germany, allow the ccTLDs referring to their territory to be delegated to private sector entities that predate any regulatory legislation, or are not regulated by any law.

Regarding internal sovereignty, the state's inability to control the delegation or operation of a ccTLD does not by itself undermine the sovereign's ability to effectively exercise control within and across its borders. One might try to challenge this assertion by saying that a ccTLD registry not controlled by the government might register Internet users and publish online content that undermines the authority of the state. This is true—but it is also true of *all* other domain names. Recall that technically, a ccTLD is no different from any other TLD. If a state's internal control is threatened by its inability to control the delegation of a ccTLD, it would also be threatened by its lack of control over the delegation of *every* top-level domain on the Internet—because unless there are filters or controls, any internet user can access those other domains and the information associated with them just as readily as it can access the ccTLD. If a state needs to assert control by blocking or regulating domains, it will have to achieve that by blocking and regulating *any* domain, not just the ccTLD operator. Indeed, the countries with the most extensive internet controls sharply regulate access to all Internet services, not just the ccTLD delegee or its policies. There is nothing special about the ccTLD; the purported linkage between information control and sovereignty is completely independent of the semantics of the top-level domain. So the argument that control of the ccTLD conveys sovereignty over information flows cannot be used to justify sovereignty claims over ccTLD delegations specifically.

2. The Semantic Isomorphism

Recall that both the DNS and the ISO-3166 list are name spaces. The ISO-3166 codes and the TLDs based on them merely *refer to* political territories; they are not the actual territories. There is a big gap between *referring* to political territories in an online name space and granting sovereigns the right to own or control actions or entities associated with the names. This should be immediately evident by considering other name spaces. Libraries routinely create classification schemes for organizing books,

periodicals and other media and it is not unusual for these schemes to use the names of countries. If a global library classification scheme created a category for, say, Portugal, would the government of Portugal be justified in asserting a right to control what objects were placed into the Portugal category, or a right to designate which librarian was responsible for classifying those materials? Most likely not. In its amicus brief in the Iran case, the U.S. government made a similar argument: "Although the right to designate its territory 'Iran' is presumably valuable to the Iranian government, no one would suggest that the name 'Iran' in an atlas or a newspaper—or even official publications—is itself the 'property' of the Iranian government . . . ."[75]

People can create name spaces that refer to states or territories without ceding control of, or incurring obligations to, the real-world referent of the name. A semantic reference to a state or its territory by a non-state actor does not by itself justify state sovereignty over the administration of the semantically related unit of a name space.

One might contend that ccTLDs are different from library classification schemes because they are, or can become, valuable enterprises to the people in a specific country. But while there is a notable isomorphism between the virtual territories created by ccTLDs and the geographic political territories of states, there is one critical difference: sovereignty is exclusive, but TLDs are *not*. There are hundreds of other TLDs accessible to any Internet user in a country. CcTLDs are not even the only TLD that can reference a given territory or country; technically, there could be dozens of TLDs that refer to the same country or territory.[76] The possibilities for including additional names referring to countries has grown with the possibility of so-called Internationalized Domain Names ("IDNs"). The original DNS standard used as its character set ASCII, an early standard for digital representation of the Roman alphabet. The ASCII character set did not allow non-Roman scripts such as Chinese, Arabic or Cyrillic to be represented. Since the early 2000s, however, the DNS standard was modified and upgraded to allow domain names in non-Roman scripts.

---

75. Brief for the United States as Amicus Curiae at 9, Weinstein et al v. Islamic Republic of Iran and ICANN., 831 F.3d 470 (D.C. Cir. 2016) (14-7193).

76. For example, in addition to the ccTLD .FR for France, there could be a TLD .FRANCE or .FRANÇAISE. There is already a .PARIS in operation: http://bienvenue.paris/en/. (last visited Mar. 27, 2017).

But this creates an ever bigger ambiguity: are IDNs that refer to a country name also ccTLDs? They refer to countries, but they are not part of the ISO-3166 list; indeed, there is no fixed list anywhere from which IDN ccTLD delegations could be drawn. Here we confront another critique of the semantic basis for the sovereignty claim. If merely using a label for a country justifies a governmental interest in controlling the names and its uses, then states would suddenly gain enormous power over a large number of words and expressions in the domain name space. The claim would extend to dozens of permutations of country names, region names, and city names. The whole point of adopting ISO-3166 as the basis for delegations was to *limit* contention about what counted as a country domain to a fixed, semi-official list. A sovereignty claim based on semantic reference takes us beyond ISO-3166 into a limitless range of names.

This slippery slope argument is not hypothetical. States already have begun to assert extensive powers over the names of geographic regions and countries in the domain name space, regardless of whether they are on the ISO-3166 list, regardless of where they are in the domain name hierarchy, and regardless of whether any existing international law supports their claim.[77] The GAC has, for example, succeeded in getting ICANN to force all new TLD registries to ask for its permission before they use any two-letter strings that match country codes in the second level of their domains.[78]

---

77. *See* GOVERNMENTAL ADVISORY COMM., THE PROTECTION OF GEOGRAPHIC NAMES IN THE NEW GTLDS (Feb. 2015), https://gacweb.icann.org/display/gacweb/Geographic+Names+in+the+new+gTLDs+process+updated+summary+and+report+-+February+2015.Summary+of+community+input. For a broader legal analysis of government claims to geographical names, *see* HEATHER ANN FORREST, PROTECTION OF GEOGRAPHIC NAMES IN INTERNATIONAL LAW AND DOMAIN NAME SYSTEM POLICY (Kluwer Law International 2013).

78. Specification 5 of ICANN's base registry contract, Scheduled for Reserved Names, Paragraph 2 states that: "All two-character ASCII labels shall be withheld from registration or allocated to Registry Operator at the second-level within the TLD. Such labels may not be activated in the DNS, and may not be released for registration to any person or entity other than Registry Operator, provided that such two-character label strings may be released to the extent that Registry Operator reaches agreement with the related government and country-code manager of the string as specified in the ISO 3166-1 alpha-2 standard." *Base Registry Agreement* (Jan. 9, 2014), http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.pdf.

3. The U.S. Role

While many early sovereignty claims were based on nothing more substantial than a quest for more power over the Internet, the special role of the U.S. government vested them with an urgency and legitimacy that they might not have had otherwise. CcTLDs were growing in value, and the owners, operators and a majority of the registrants were usually based in the country's jurisdiction. The power to redelegate a ccTLD—to take away the name or delegate it to someone else—was literally the power to destroy these enterprises. While the U.S., as far as we know, never used its control of ICANN overtly as an instrument of foreign policy, much less to intervene in the internal affairs of other countries, the fact remained that its control of the DNS root gave it the *capability* to do so. As the Internet and ccTLD registries became a larger and more important part of a country's (and the world's) digital economy, the idea that the U.S. government retained supreme authority over their very existence rankled other states, allies as well as enemies.

The World Summit on the Information Society ("WSIS"), an intergovernmental UN Summit that took place between 2002 and 2005, formally ratified states' disgruntlement with this situation.[79] Its concluding document, the *Tunis Agenda*, stated:

> Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanism.[80]

Paradoxically, in order to justify its special role, the U.S. government had to acknowledge and recognize the sovereignty concerns of other states. In a 2005 statement issued during the WSIS proceedings, the U.S. reasserted its intention to retain "its historic role in authorizing changes or modifications to the authoritative root zone file," but it also recognized that

---

79. *See generally* MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE Chap. 4 (2010).

80. World Summit on the Information Society, *Tunis Agenda for Information Society* ¶ 63 (Nov. 18 2005), http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

"governments have legitimate public policy and sovereignty concerns with respect to the management of their ccTLD."[81]

Thus, the most realistic and practical justification for sovereignty claims over ccTLDs was the fact that one sovereign (the United States) possessed ultimate control over all ccTLD delegations, and other countries needed to assert sovereignty to check and balance that control. But U.S. control of the root is a historically contingent situation, not an inherent or permanent feature of Internet governance. In 2014, the U.S. Commerce Department announced its intention to end that arrangement and turn over control to ICANN and the "global multistakeholder community,"[82] and the transition was successfully carried out on October 1, 2016. If sovereignty claims are justifiable as a reaction to that contingency, the end of U.S. control of the root eliminates one of the primary drivers of sovereignty claims.

Today, the perception of a linkage between the ccTLD and sovereignty is based on nothing more substantial than a semantic reference and the strong (but imperfect) isomorphism between the ISO-3166 codes and political territories. In some ways this isomorphism became a self-fulfilling prophecy. By creating a unique and exclusive code for each territory, the ISO-3166 list fueled a misguided perception of an intrinsic linkage between the territorial state and the top-level domain. As the Internet grew and control of TLDs became economically and politically significant, this isomorphism interacted with the innate tendency of governments to try to control whatever they can control. The *coup de grace*, however, came from the international politics associated with the birth and evolution of ICANN. The U.S. government had unilateral authority over ICANN and IANA, which made other states invoke sovereignty as a defense against potentially arbitrary U.S. actions against them in that space. In order to gain their acceptance of the regime, the U.S. had to reassure other states that its indirect control of the DNS root via ICANN would respect their sovereign sensitivities and aspirations.

---

81. National Telecommunications and Information Administration, *U.S. Principles on the Internet's Domain Name and Addressing System* (June 30, 2005), http://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system.

82. National Telecommunications and Information Administration, *NTIA Announces Intent to Transition Key Internet Domain Name Functions* (Mar. 14, 2014), https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions. *See also* IANA, *Overview*, Stewardship Transition Coordination Group, (Mar. 28, 2017), https://www.ianacg.org.

C. Property Rights Theory and ccTLDs

Having shown that sovereignty does not provide a guiding principle for global governance of TLDs, we turn now to an alternative governance mode, the recognition of property rights and markets in ccTLD delegations. As alluded to before, in the Iran controversy and elsewhere, the claim that TLD delegations can be property is highly controversial. Yet someone approaching the topic from the standpoint of law and economics theory might have trouble understanding why. In general a property right has four key characteristics:[83]

1. The right to use and control something;
2. The right to the benefits or revenues generated by it;
3. The right to exclude others from either use or benefit;
4. The right to transfer or assign to others.

Each of these four aspects of a property right applies to the assignee of a domain name, regardless of whether the assignee holds a TLD or a second level domain.

D. Property Rights and Domain Names

Domain name registrants gain an exclusive right to use a globally unique character string.[84] The right to use a unique character string as an Internet address also means that the registrant can exclude all others from registering or operating the same name. Indeed, the right to exclude is essential to the performance of the domain name's technical function. Domain names must be globally unique to serve as an Internet address; similar to phone numbers, once a domain name is assigned to one person it should not be assigned to anyone else. Exclusivity also means that the registrant acquires a right to the benefits or revenues associated with the domain or the services that use the domain as an address. The domain name registrant can, and often

---

83. Harold Demsetz, *Some Aspects of Property Rights*, 9 J. L. & ECON. 61, 61–62 (1966); *see also* Armen A Alchian, *Some Economics of Property Rights*, 60 IL POLITICO 816 (1965); Eirik Grundtvig Furubotn & Rudolf Richter, INSTITUTIONS AND ECONOMIC THEORY: THE CONTRIBUTION OF THE NEW INSTITUTIONAL ECONOMICS (University of Michigan Press 2005); David W Pearce, MIT DICTIONARY OF MODERN ECONOMICS 351 (MIT Press 1992).

84. In the domain name industry, a 'string' refers to a unique set and order of alphanumeric characters.

does, sell or transfer the name to others at a market price, or lease out subunits of the property (lower-level domain names) for money.

A book by the legal scholar Konstantinos Komaitis argues for the "legal autonomy" of domain names with respect to trademarks, concluding that they are intangible property rights with substantial value that can be bought and sold, and are subject to property-oriented *in rem* jurisdiction.[85] Domain names' lack of physicality does not alter their status as property; even for physical goods, property is widely considered a "bundle of rights" that administer the relationship between the owner and the other individuals in reference to the property.[86]

Thus, it is evident that a domain name registration provides its registrant with 1) the right to use and control it; 2) the right to reap monetary or other rewards generated by its use; 3) the right to exclude others from use and benefit; and 4) the ability to sell or transfer the name.

E. ICANN's Arguments in the .IR Case

With law and economics theory providing a strong presumption that domains are property, we now turn to the litigation over .IR, and examine ICANN's argumentation.[87] In this case, victims of state-sponsored terrorist acts sued, and succeeded in winning a judgment against, the governments of Iran, Syria and North Korea. In an attempt to enforce those judgments, the judgment creditors started looking for property belonging to the respective governments that they could attach. One of the few potentially attachable properties they could find outside those countries' sovereign jurisdictions were ccTLD delegations and blocks of Internet protocol addresses. Viewing ICANN as a third-party garnishee, plaintiffs then sued ICANN to obtain the ccTLDs and IP numbers.

As the target of the lawsuit, ICANN strongly resisted the plaintiffs' attempts to attach the .IR delegation. The key issue being litigated was not a ccTLD's property status *per se*, but the ability of the plaintiffs to seize the delegation as judgment creditors.

---

85. *See* KONSTANTINOS KOMAITIS, THE CURRENT STATE OF DOMAIN NAME REGULATION: DOMAIN NAMES AS SECOND CLASS CITIZENS IN A MARK-DOMINATED WORLD 58–59 (2010) (discussing the 9th Circuit Court of Appeals decision in the sex.com case).

86. Morris R Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 12 (1927).

87. Motion to Quash Writ of Attachment, *supra* note 17.

Nevertheless, ICANN's argument rested heavily on contesting the notion that a ccTLD was property. It argued that:

1. ccTLDs are not property;
2. Even if ccTLDs are property, they are not attachable in the District of Columbia;
3. Even if they are attachable, ICANN cannot transfer them unilaterally;
4. Even if ICANN can transfer them, doing so would wreak havoc on the Internet;
5. Defendants do not own the ccTLD;
6. Even if the defendants own the ccTLDs, the Foreign Sovereign Immunity Act applies and ICANN cannot hand it over.

In the analysis below, we touch on all of these arguments except (3), which is not relevant to the thesis of this paper. Argument (2), as we shall see, is the one that actually won the case in the District of Columbia Court and is taken up in section 5b below. Argument (4) is what won the case in the U.S. Court of Appeals for the District of Columbia Circuit and is discussed in section 5e. Note that in argument 6), the issues of property and sovereignty converge.

ICANN put forward several reasons why a ccTLD cannot be considered property. One of the more tenuous was that a ccTLD "cannot be physically held." While it is true that domain names are not physical objects, all legal regimes recognize the existence of intangible property, such as trademarks or copyrights. ICANN also tried to assert that ccTLDs are not property because ccTLD managers are unable to exclude. "The entire premise of a ccTLD," ICANN argued, "is that it will be used and enjoyed by many who choose to register, operate and visit domain names within that ccTLD."[88] ICANN's argument about exclusivity is both conceptually muddled and empirically false. It is muddled because it confuses the exclusivity of property ownership with technical configurations of the domain that would exclude the general public from seeing or accessing lower-level domains once they are leased to and made operational by the ccTLD's customers. The latter is not the kind of exclusivity to which property rights theory refers (and it is unclear why any registry that sells domains to the public would want to do that).[89] Exclusivity refers to the ability of an

88. *Id.* at 14.

89. CcTLD delegations are, in fact, based on an agreement that secures their exclusivity. In some cases, this is a contract, in others it is a formally

owner to withhold a good or service from use by others until the owner is offered something of value in return. In fact, ccTLD owners can and do exclude in this sense. Nearly all ccTLDs require payments to use a domain, and thus exclude people who do not pay them from registering and using a domain in their TLD. Additionally, many ccTLDs set policies that limit domain name registration to organizations with a physical presence in their territory, thus excluding certain classes of users from registering under the domain.

In its attempt to deny the property status of ccTLDs, ICANN argued that a ccTLD has "no intrinsic value" but is merely "a collection of technical and administrative services."[90] But this argument ignores the intrinsic value of the actual TLD name registration in the root zone. Registry operations do involve several technical and administrative services that make the domain and any registrations below it functional on the Internet. But unless that "collection of technical and administrative services" is anchored in a unique ccTLD registration in the root zone, the registry service is worthless. In other words, without the exclusive right to use a unique TLD character string, a registry cannot offer the public functional, globally unique second-level domain names. Thus, registration and control of a globally unique character string, such as a two-letter ccTLD, is an indispensable component of a domain name registry service. Saying that a ccTLD delegation has no intrinsic value because it requires supporting services such as Internet access and servers is like saying a computer has no intrinsic value because it does not work without electricity or software.

ICANN argued that a ccTLD "is not capable of precise definition" because it is "constantly changing as new domain names are added and deleted."[91] We would argue the opposite: a ccTLD's definition is quite simple and precise: it is the unique character string that is registered in the root. While it is true that new second-level and third-level names under a ccTLD can be constantly added and old ones deleted, all of these subdomains are contractually derived features of the registry's ownership of the top-level domain. Other forms of property have analogous

---

documented delegation decision of the IANA. In other cases, the delegation decision predates IANA record-keeping, but in all cases the exclusive assignment is manifested in IANA's Whois records and the contents of the root zone file.

90. Motion to Quash Writ of Attachment, *supra* note 17, at 10.

91. *Id.*

characteristics. The owner of real estate, for example, can change the value of the property by building one or more dwellings and leasing them out. The number of rental units on a single piece of real property can always change and so can the people in them. These changes in a rental property do not change its boundaries, its definition, or its status as property.

Most implausibly, ICANN argued that "there is no established market within which a ccTLD can be purchased or sold."[92] But in fact, both generic and country code top-level domains have been bought and sold. In its recent round of adding new top-level domains, ICANN itself organized an auction market to determine who would receive TLD names for which there were multiple applicants.[93] The .CC country code domain was purchased by Verisign, the company that operates the .COM registry, through a merger agreement with its original delegee in 2002. In an auction held by the government of Montenegro, the company DoMEN Ltd. won the auction to operate the ccTLD .ME.[94]

In its attempt to deny that ccTLD operators own their domains, ICANN appealed to "authoritative Internet protocol standards and the views of governments around the world," which allegedly deny property rights to delegees. The "authoritative" standards to which ICANN refers are RFC 1591 and ICP-1, both discussed at some length in section 3 above. Neither of them are protocol standards, and, even if they were, they would not be binding.[95] ICP-1 is a policy document issued unilaterally by ICANN in 2000 that was never accepted as binding policy by ccTLD managers and was formally abandoned in 2015. By "the views of governments," ICANN refers to the GAC Principles, which constitute *nonbinding* policy advice issued by its Governmental Advisory Committee.[96] The GAC Principles merely express the policy preferences of the

92. *Id.*

93. See, *New GTLD Program Auctions: Understanding Auctions* (Aug 17, 2015), https://newgtlds.icann.org/en/applicants/auctions.

94. DoMEN Ltd. is a Montenegrin joint venture founded in 2008 by Afilias Limited, GoDaddy.com and ME-net, Ltd that does business as a .ME Registry. *See .ME As a Company*, http://domain.me/me-as-a-company/(last visited Mar. 30, 2017).

95. RFC 1591 classifies itself as "informational" and says, "This memo does not specify an Internet standard of any kind." Postel, *supra* note 32. At any rate, all IETF standards are voluntary.

96. The GAC Principles say: "No private intellectual or other property rights should inhere in the ccTLD itself, nor accrue to the delegee as the result of the management, administration or marketing of the ccTLD." GAC, *Principles for Delegation and Administration of ccTLDs* (Feb 23, 2000), https://archive.icann.org/en/committees/gac/gac-cctldprinciples-23feb00.htm.

GAC; they are not legally binding rules, nor are they scientifically grounded findings about the property status of ccTLDs. GAC statements are not even binding upon ICANN itself.[97] The fact that many governments do not want property rights to inhere in a ccTLD doesn't prove that it is illegal, impossible or harmful for there to be such rights.

In argument (6)—that the domain cannot be attached because of the Foreign Sovereign Immunities Act (FSIA)—ICANN contended that the property of a sovereign cannot be attached unless it is used for commercial activity in the foreign jurisdiction.[98] The convergence of the property and sovereignty issues might raise two complex factual issues: whether IRNIC, the organization that runs the .IR ccTLD, is an arm of the Iranian state or not,[99] and, if so, whether IRNIC's sales of domain name registrations under .IR constitute the kind of commercial activity in the U.S. that would eliminate the sovereign immunity granted by the FSIA.[100]

Section 1605A of the FSIA, however, creates a much broader exception to a foreign sovereign's general jurisdictional immunity for cases involving terrorism. When the foreign state has been designated as a state sponsor of terrorism at the time the terrorist act occurred, the state's immunity from money damages is abrogated, and the foreign property becomes subject to attachment regardless of:

A) The level of economic control over the property by the government of the foreign state;

B) Whether the profits of the property go to the government;

---

97. *Bylaws for Internet Corporation of Assigned Names and Numbers* § 2.1 (j)-(k) (Oct. 1, 2016), https://www.icann.org/resources/pages/governance/bylaws-en/ (making clear that the ICANN board can decide not to follow the GAC's advice).

98. Motion to Quash Writ of Attachment, *supra* note 17, at 18.

99. IRNIC, which is run by Institute for Research in Fundamental Sciences (IPM), argues that it is an educational institution independent of the state. Weinstein v. Islamic Republic of Iran, 831 F.3d 470, 482 (D.C. Cir. 2016). However IPM is affiliated with and sponsored by the Iranian Ministry of Science, Research and Technology. It is not clear where the money from selling .IR domain names goes.

100. Similarly, in Rubin v. Iran, 830 F.3d 470 (7th Cir. 2016), Plaintiffs sought to attach ancient Persian artifacts held by the University of Chicago and the Field Museum of Natural History. Similar to the .IR case, plaintiffs alleged that these artifacts are the property of Iran and are subject to attachment in satisfaction of their judgment under either section 201 of TRIA or the attachment provisions of the FSIA, 28 U.S.C. §§ 1609, 1610.

C) The degree to which officials of that government manage the property;
D) Whether that government is the sole beneficiary in interest of the property; or
E) Whether establishing the property as a separate entity would entitle the foreign state to benefits in U.S. courts.[101]

Not surprisingly, the D.C. Circuit Appeals court decisively rejected ICANN's argument about the FSIA, noting that "once a section 1605A judgment is obtained, section 1610(g) strips execution immunity from *all* property of a defendant sovereign."[102]

Based on the analysis above, ICANN's arguments about the property status of ccTLDs do not stand up. But ICANN won its case in the district court for a different reason. The court ruled that, even if ccTLDs are property, they are not attachable under District of Columbia law.[103] And in the appeals court, defendant ICANN prevailed because of the court's concern about the impact of a "forced redelegation" of a ccTLD on third parties.[104] As the next section will show, the case law regarding domains as property often turn on issues that do not directly rule on the property status of domains, but consider the broader implications of a legally required seizure of the property.

A. Property or Service? The Legal Debate

While applications of legal and economic theory make a compelling case for domain names as property, the fact remains that litigation on the property status of domain names has been taking place for nearly 20 years, with less than settled results. In this section we will discuss some of the most important cases worldwide that directly or indirectly dealt with the matter of domain names' property status. Contrary to popular opinion, most of these cases do not classify domain names as services rather than property; instead, they usually find that their status as property is not relevant to the question of whether they can be attached.

It is important to note that these disputes are usually between the TLD registries and their customers, registrants of second-level domains, or between the registry and someone making a claim

101. 28 U.S.C. § 1610(g).
102. Weinstein, 831 F.3d at 483.
103. Stern v. Islamic Republic of Iran, 73 F. Supp. 3d 46 (D.D.C. 2014).
104. *See infra* section 5.e.

against one of its registrants. In these cases, the *top-level* domain registries vehemently argue against recognizing *second-level* domain names as property rights, just as ICANN, the *root zone* registry, argues vehemently against recognizing *top-level* domains as property. We will argue that these conflicts are more about *whose* property rights are more important than about *whether* property rights are involved. Our analysis will clarify both the courts' approach to the issue of domain name as service or property and why registries tend to oppose affording property rights to entities below them in the naming hierarchy.

In most of the common law cases, domain names have been ruled to be property. In *Kremen v. Cohen*, the United States Court of Appeals for the Ninth Circuit held that a domain name is intangible property because it satisfies a three-part test for the existence of a property right: it is an interest capable of precise definition; it is capable of exclusive possession or control; and it is capable of giving rise to a legitimate claim for exclusivity.[105] Other common law jurisdictions have also treated domain names as intangible property. In India, in *Sayam Infoway*, the Supreme Court held that a domain name can be recognized as intellectual property and subject to trademark law.[106]

In the UK, in *OBG Ltd. v. Allan,*[107] Lord Hoffman observed that "I have no difficulty with the proposition that a domain name may be intangible property, like a copyright or trademark."[108] In Australia, in *Hoath v. Connect Internet Services Pty. Ltd.*,[109] the judge stated that "[t]he internet registrar gave Mr. Hoath the exclusive right to use the domain name dragon.net.au, the IP addresses and the AS number. I will assume, without deciding, that Mr. Hoath had a right in property. Undoubtedly it was a valuable right." In Canada, an Ontario Superior Court of Justice decision confirmed that domain names under the .CA ccTLD are personal property and are accordingly subject to the rules that govern any other type of personal property.[110] In *Tucows.Com Co v. Lojas Renner S.A*, the court concluded that "Tucows has a bundle of rights in the domain name that

105. Kremen v. Cohen, 325 F.3d 1035 (9th Cir. 2003).

106. Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd. (2004) 2 S.C.R. 465 *at* ¶¶ 11–12 (reporting a decision Supreme Court of India).

107. OBG Limited v. Allan [2007] UKHL 21 [appeal taken from Eng.].

108. *Id.* at ¶ 101.

109. Hoath v. Connect Internet Services [2006] NSWSC 158 (citing a case from the New South Wales Supreme Court in Australia).

110. Mold.ca Inc v. Moldservices.ca Inc (2013) (Ont. Sup. Ct. of J.) No.CV-13-480391.

constitutes personal property within the meaning of Rule 17.02 (a)."[111] In the UK, a court of first instance ruled that domain names were not goods, but the court of appeal adjourned an application for permission to appeal and it did not decide whether an Internet domain name constituted 'goods' or not.[112] In the ICANN/Iran case, the first D.C. Circuit ruling quashing the motion for a writ of attachment of .IR also did not resolve the property issue. The court concluded that the ccTLD was not subject to attachment under District of Columbia law.[113] It did not, however, reject the proposition that ccTLDs are property; in fact, it stated "the conclusion that ccTLDs may not be attached in satisfaction of a judgment under D.C. law does not mean that they cannot be property."[114]

Other court decisions have explicitly classified domain name registrations as a property right. In a case involving a trademark-domain name conflict in Germany, the European Court of Human Rights asserted that the concept of "possession" is not only limited to ownership of physical goods but also applies to intangible goods such as domains. The court stated that the contract between the registrar and the registrant gave an open-ended right to the domain name holder to benefit from the revenue it generated, sell the right to others and exclude others from use of the domain. "The exclusive right to use the domains in question thus had an economic value. Having regard to the above criteria, this right therefore constituted a 'possession'."[115] The same argument was put forward by the Virginia Circuit Court in *NSI v. Umbro* before the judgment was reversed by the Virginia Supreme Court.[116] In a Swedish case, the prosecutor moved that the domain names piratebay.se and thepiratebay.se should be confiscated as they were being used to violate the Copyright Act; the district court found that a domain name should be considered as intangible property and subject to confiscation.[117]

---

111. Tucows.com Co. v. Lojas Renner S.A. [2011 ONCA 548 Ct. Ap. Ont.] (reporting a decision of the intermediate appellate court of the province of Ontario).

112. The Honourable Nicholas Augustine Plant v. Service Direct, [2006] EWCA (Civ) 219 (reporting a decision of the court of appeals for England and Wales).

113. Motion to Quash Writ of Attachment, *supra* note 17.

114. *Id.* at 8 n.2.

115. Paeffgen GmbH v. Germany, 8-9 Eur. Ct. H.R (2007).

116. Network Sols., Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80 (Va. 2000).

117. Tingsratt [TR] [District Court] 2015 B 6463-13 (Swed), *https://www.iis.se/docs/Stockholms-TR-B-6463-13-Deldom-2015-05-*

There is a widespread assumption that several key U.S. cases have classified domain names as a contract for service between the registrar and the registrants. That assumption is incorrect. In the past, courts did not directly classify domain names as services; they usually found that the question of whether domain names are property or service is immaterial to the outcome of the case. This is what actually happened in *Network Solutions, Inc. v. Umbro International,* one of the cases most commonly cited to prove that domain names are services. The court indicated that "a domain name registration is the product of a contract for services between the registrar and registrant."[118] Howesver, it held that whatever contractual rights the registrant has, even if they involve property, do not come into existence without the NSI service, and a contract of service cannot be subject to garnishment.

Garnishment is a creature of statute, not common law, and the *Umbro* court was concerned that its ruling should strictly satisfy the criteria of the statute. If it allowed the garnishment of the NSI service, the court argued, any contract for service would be garnishable, which the court was not willing to allow without statutory change. While the court discussed the property rights vs. service aspect of the domain name, in the end it concluded that ascertaining whether domain names are an intellectual property right would not affect the outcome of the case.[119] Hence it did not make an affirmative judgment on the property status of domain names. In *Dorer v. Arel*, the court provided reasons to *doubt* whether domain names can be treated as personal property subject to lien. But in the end, without making any conclusion on the legal classification of domain names, the court decided that the dispute should be resolved based on the dispute resolution policy of the .COM registry.[120]

19_avidentifierad.pdf. The Stockholm District Court had ruled that the registry (.SE provider) is not liable for the act of infringement of the domain name owner. The prosecutor appealed the District Court's decision. The appellate court decided that the registry (.SE) does not have any ownership rights over domain names and upheld the district court decision that domain name is property but the .SE registry is not liable for the actions of the domain name owner. It asserted, "Instead, the assessment of the Court of Appeal is that the right to a domain name, which carries a possible economic value, comprises a form of intellectual property."

118. Network Sols., Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80 (Va. 2000).

119. *Id.* at 85.

120. Dorer v. Arel, 60 F. Supp. 2d 558, 561 (E.D. Va. 1999) ("In any event, the knotty issue of whether a domain name is personal property subject to the lien of *fieri facias* ultimately need not be resolved because there is a more

There is one case in which the court did decide that domain names were a service—but the reasoning was based on an error. In *Lockheed Martin Corp. v. Network Solutions*,[121] when asked to decide whether the .COM TLD provides a service or a product, the court decided that the manager of .COM provided a service:

> NSI's role [as the manager of .COM] differs little from that of the United States Postal Service: when an Internet user enters a domain-name combination, NSI translates the domain-name combination to the registrant's IP address and routes the information or command to the corresponding computer . . . NSI does not supply the domain-name combination any more than the Postal Service supplies a street address.[122]

The court's argument that NSI "does not supply the domain name combination" is factually incorrect. A TLD registry is without question the source and supplier of the domain name combination that users register. Contrary to the opinion in *Lockheed Martin*, NSI is more than a post office that delivers traffic to a domain—it does indeed supply the street address. The registration of a new TLD such as .COM creates a supply of second-level domain names under it, and one of a TLD registry's chief technical functions is to keep track of which names have been occupied and which are available. The court's ignorance of the technical functioning of DNS seems to have contributed to its conclusion in *Lockheed*.

In the debate about domain name as property or service, the registries almost always argue against domain names as property. Why has this happened? One very important reason is that the TLD registries are, in effect, asserting that *they* control the name space under their TLD, and the rights registrants possess are only those granted to them by the TLD's contract for service. Recognizing second-level domain names as property might undermine the registries' exclusive possession over the name space created by its TLD. This approach is also obvious in their terms and conditions. For example, .AU, in its policy for allocation of domain names, clearly states that registrants do not own a domain

---

readily available, practical solution to the problem to be found in NSI's policies.").

121. Lockheed Martin Corp. v. Network Sols, Inc., 194 F.3d 980 (9th Cir. 1999).

122. *Id.* at 984–85.

name.[123] The terms of service of Nominet, the .UK registry, explicitly states that domain name registrants have no property rights over their domain name.[124]

In *NSI v. Umbro*, NSI (the owner of the .COM TLD) argued that NSI's registration services agreement was the only source of rights acquired by a registrant and that a "registrant receives only the conditional contractual right to the exclusive association of the registered domain name with a given IP number for a given period of time."[125] In *Zurakov v. Register.com*,[126] the plaintiff claimed that his registration of the domain name "laborzionist.org" entitled him to property rights and that the registrar did not have the right to use the name and the website for its own advertisement displayed on a "Coming Soon" page. The defendant, a registrar, argued that it provided a contract for services which did not allow the defendant the exclusive use and control of the domain name and that this has been also stated in its policy on the website. The registrar assumed that it had the authority to limit the rights of the domain name holder and also make changes to the website of the domain name holder when it was inactive.

To summarize: by arguing that they are merely providing a contractual service to domain name registrants, the TLD registry strengthens its own property rights and weakens those of the registrant. With respect to the property/service debate, we conclude that domain name registries supply a contracted service to users, but this does not undermine the property status of a top-level domain. The possession of a unique top-level name registration is an essential input to the provision of a registry service. While it is true that a TLD registration needs to be supported by ancillary services such as Internet access and name resolution servers to fulfill its function as an Internet address, it is also true that the ancillary services would be completely worthless unless they are anchored in a globally unique and exclusive

123. *Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs*, section 2.1 (Apr. 2012), https://www.auda.org.au/pdf/auda-2012-04.pdf/. "There are no proprietary rights in the domain name system (DNS). A registrant does not 'own' a domain name. Instead, the registrant holds a licence to use a domain name, for a specified period of time and under certain terms and conditions."

124. *Terms and Conditions of Domain Name Registration*, section 10 (Sep. 2015), http://www.nominet.uk/wp-content/uploads/2015/10/Terms_and_Conditions_of_Domain_Name_Registration_1_Sept_2015.pdf.

125. Network Sols Inc. v. Umbro Int'l, Inc., 529 S.E.2d 80 (Va. 2000).

126. Zurakov v. Register.Com, Inc., 760 N.Y.S.2d 13 (N.Y. App. Div. 2003).

domain name registration. Because domain name functionality involves both property and service, court decisions denying a plaintiff's right to garnish a service could be correct in a particular jurisdiction, depending on its laws regarding the attachment or garnishment of property, without necessarily undermining the property status of the domain name registration itself.

B. The Appeals Court Decision in the .IR Case

The latest decision in the ICANN case departed sharply from prior legal precedents. The court looked beyond the narrow issue of whether the .IR ccTLD was attachable property. It assumed, "without deciding," that "the ccTLDs the plaintiffs seek constitute 'property' under the Foreign Sovereigns Immunity Act and, further, that the defendant sovereigns have some attachable ownership interest in them."[127] Thus ICANN's weak arguments against the property status of TLDs had no impact on the decision. Instead, the court refused to allow the .IR domain to be seized because

> the court has the "authority" to "prevent appropriately the impairment of an interest held by a person who is not liable in the action giving rise to a judgment"—i.e., we are expressly authorized to protect the interests of ICANN and other entities. Because of the enormous third-party interests at stake—and because there is no way to execute on the plaintiffs' judgments without impairing those interests—we cannot permit attachment.[128]

One of the third-party interests at stake would be that of the second-level domain name registrants under .IR, most of whom were not guilty parties in the terrorist act. Their Internet access might be severely harmed or even eliminated if control of the top-level domain was shifted to the plaintiffs. But the court seemed particularly concerned about the impact of a decision for the plaintiffs would have on ICANN's ability to maintain the stability and interoperability of the DNS.[129] By "requiring ICANN to delegate '.ir' to the plaintiffs," the court opined, the plaintiffs

---

127. Weinstein, 831 F.3d at 485.

128. *Id.* at 485–86.

129. *Id.* at 486 ("even if the plaintiffs are able to show adequate competence and commitment [to operate the .IR top-level domain], the act of forced delegation itself impairs ICANN's interest in "protect[ing] the stability . . . [and] interoperability . . . of the DNS").

"would bypass ICANN's process for ccTLD delegation" and this would have a harmful impact on the global DNS and on ICANN itself.[130] Indeed, the court cited approvingly an amicus brief from the U.S. government that asserted that "the result [of a forced redelegation] would be devastating for ICANN, for the model of Internet governance, and for the freedom and stability of the Internet as a whole."[131]

The principle that attachments or seizures of property rights can be limited or stopped due to their impact on third parties is a good one, and consistent with law and economics theory regarding externalities and the proper assignment of liability.[132] The motivation for the court's interest in the impact on ICANN's role in Internet governance, however, is much less clear. The court did not go into detail about how or why bypassing ICANN's delegation process constituted an impairment of *ICANN's* interest in a stable and globally compatible DNS, but one can infer from its discussion that it feared a redelegation of .IR to Israeli terrorism victims might cause Iran to abandon the ICANN regime altogether and thereby risk a split in the DNS root.[133]

Here the court departed from the world of legal analysis and entered the world of geopolitics and the political economy of Internet governance. It is true that, insofar as this internet governance regime imposes limits on the authority of sovereigns, it creates some risk of a national defection from the institutional and technical arrangements that ensure global compatibility of Internet communications. An American court ordering the seizure of the ccTLD of a nation-state with a longstanding hostility towards the United States would indeed inflame geopolitical tensions.

In assessing that risk, however, one must bear in mind the constraints on state action. The practical benefits of Internet connectivity for any given country are great, and the costs of severing it would be very high. It is noteworthy that, despite more than a decade of complaints about the special U.S. role in DNS governance and systematic and very expensive efforts by sovereignty-oriented governments such as Russia, China and Iran to protect themselves from free expression on the Internet, none of them have formed a competing DNS root, nor have any of them

130. *Id.*

131. *Id.*

132. Antonio Nicita & Matteo Rizzolli, *Property Rules, Liability Rules and Externalities*, 24 J. PUB. FIN. & PUBL. CHOICE 2–3 (2007).

133. *See* Weinstein, 831 F.3d at 487–88 nn. 31–33.

even come close to cutting themselves off from the Internet completely.

The appeals court decision, then, did not make a decision about the property status of domains, nor did it weigh in on the viability of sovereignty claims over ccTLD delegations, other than to reject ICANN's claim that the FSIA negated the property claim. What it did was bolster the public trustee model of ccTLD delegation, by establishing a legal precedent that ICANN's role as global steward of domain name delegations somehow depends on preventing a ccTLD redelegation decision that bypasses ICANN's normal process.

5. PROPERTY, SOVEREIGNTY AND PUBLIC TRUSTEE: FOUR GOVERNANCE SCENARIOS

In this section, we explore the broader global governance implications of treating ccTLD delegations according to principles of sovereignty, property rights or public trusteeship. Our analysis indicates that we do have a choice of governance arrangements. We have shown that there is no legal, political or logical basis for a sovereignty claim over ccTLD delegations—nevertheless, governments have succeeded in gaining a major degree of influence over delegations of ccTLDs that refer to their country. Similarly, we have refuted claims that TLD registrations cannot be a form of property, or function economically as property rights.

Nevertheless, we have shown that governments and regulatory institutions such as ICANN and the courts can and do impose limits on what people can do with their domains; either contractually or by imposing trustee obligations on the delegees. This means that the choices we face in our treatment of ccTLD governance are not predetermined by the laws of engineering, economics or physics but are *policy choices*. In other words, we can, if we wish, choose to make ccTLD delegations more or less subject to sovereignty claims, and we can, if we wish, strengthen or limit the property rights of ccTLD delegees. Ideally, these choices would be based on an understanding of what kind of consequences the choices would bring; i.e., how would the choices affect the efficiency and equity of global Internet governance. Of course, the different policy choices have different levels of political feasibility. But it is worthwhile to consider first the merits and drawbacks of the options based on an abstract assessment of their likely consequences.

For analytical purposes, we can reduce the basic options available for ccTLD governance to the simple 2 by 2 matrix below (Table 1). On one dimension, sovereignty over delegations can

Table 1: Governance Scenarios

	Property right	Public Trustee
Sovereignty rights over delegation recognized	A (Mercantilist)	B (PTT model)
No sovereignty rights recognized over delegation	C (Free trade)	D (RFC 1591)

be recognized or rejected; on the other dimension, the ccTLD delegation can be considered a private property right of the delegee, or it can be conceived as a public trustee. Table 1 is not intended to be a classification scheme into which all existing ccTLD arrangements can be placed. It is rather a forward-looking framework for normative assessment of the different policy options. It provides a basis for analyzing and assessing the merits and demerits of recognizing or refusing to recognize sovereignty and property rights over ccTLD delegations.

Sovereignty here means sovereignty over *delegations* or *redelegations* by IANA; i.e., whether governments have the unalloyed right to dictate who occupies and administers the ccTLD string semantically associated with their territory. It is *assumed* that states can and will regulate the conduct of any domain name registries and registrants subject to their jurisdiction, as part of their normal domestic sovereignty. Domestic sovereignty would not, however, necessarily give states the right to compel ICANN to delegate or redelegate the ccTLD string to a particular individual or organization.[134]

134. The line could blur: if a state deems a particular delegee undesirable (e.g., due to criminal or politically unacceptable behavior) they might be able to

The other dimension in the matrix refers to the extent to which the delegee has property rights over the ccTLD string. The property rights column means that the delegee has the right to develop the TLD in any way it wishes, and a great deal of freedom to subcontract, re-assign or sell the delegation. The public trustee column means that the delegee's claim on the delegation is contingent upon some external authority's determination that it is the appropriate holder, and usually involves obligations to a community and major restrictions on transferability. We have given names to each of the four options created by this matrix, which may help to clarify what they mean.

In **Option A**, both state sovereignty over delegation and the holder's private property right over the ccTLD are recognized. This we call the *Mercantilist* option. The state controls the delegation but awards it as a private property right to a privileged operator to exploit at will, in a fashion analogous to the letters patent or trading monopolies awarded to private actors in mercantilist economies. The state's ongoing authority to redelegate, however, means that the operator is beholden to it and, in that respect, is still constrained in its use of the property.

In **Option B**, sovereignty is recognized but the state treats the delegation as a public trustee and instrument of national policy. We call this the PTT model because of its similarity to the institutional arrangements surrounding the Post, Telephone and Telegraph monopolies of the 20th century. In this model, the ccTLD can be owned and operated by the state as most PTTs were, or delegated to a highly regulated and supervised private or quasi-public actor, as is done in the U.S. and Australia. The state would subject the delegee to specific obligations and limit the exercise of the right to operate the domain in accordance with those requirements. The state would also eliminate the delegee's ability to transfer the right to another party.

In **Option C**, sovereignty is not recognized and delegation involves the grant of a property right. The ccTLD (like commercial gTLDs) can be managed according to the preferences and profit of the delegee, and the delegee has a great deal of freedom to trade or transfer the delegation. We call this the *Free Trade* option. It does not put ccTLDs in a special category distinct from the global domain name market as a whole, but recognizes them as suppliers

---

eliminate them from eligibility, force a redelegation, and then strongly influence the options available in the redelegation process.

of registry services that, in principle, compete with any and every other TLD registry.

In **Option D**, sovereignty is not recognized, but delegees are considered public trustees. This would mean that a non-state actor such as ICANN (or some other global authority or institution) decides on delegations, and enforces the public trustee obligations through contracts. We call this the *RFC 1591* option, because it corresponds to the policy framework articulated by Jon Postel in RFC 1591.

A. Sovereignty

Pure sovereignty over the ccTLD means that the recognized government of a country has, at any moment, the power to redelegate the ccTLD domain to whomever it wishes, and the global root zone administrator passively complies with those wishes. Recognizing sovereignty means that the state can act unilaterally, and ignore the wishes of other domestic stakeholders as well as the global Internet community, in delegating or redelegating the ccTLD domain. One possible benefit of a sovereigntist model is that the criteria for delegation and the policies adopted by ccTLDs would reflect the diversity of the world's political regimes. That diversity and decentralization cuts both ways, however. In states with stable societies and rule of law, the downsides of state control will be limited by due process constraints and democratic accountability. If the local government is unstable, dictatorial or corrupt, the country domain's management will reflect those political pathologies. Recognizing sovereignty could easily devolve into a mercantilist or clientelist model, in which the delegation is, despite nominal public control over who gets the delegation, a de facto property right for government cronies, or for the government itself. Instability in delegations caused by shifting political winds could undermine investment, quality of service and freedom of information. In countries with ccTLDs that have already been delegated to private actors, granting the sovereign total control over delegation would significantly increase the power of the state to exert political pressure on an incumbent ccTLD operator by creating an open-ended threat of expropriation should its policies and operations not conform to the wishes of the state. In undemocratic societies this can have extremely negative consequences.

In democratic countries, a sovereigntist approach to ccTLD delegation is more likely to take the form of option B, the PTT model. This would encourage making the domain an instrument of

national policy, like the classical PTT or a public broadcaster. Yet a PTT model seems inappropriate for Internet domains, because unlike the physical telecom infrastructure, top-level domains are virtual resources that are not exclusive to one territory but potentially available in all territories. Furthermore, there are very few constraints on the creation of new TLDs that could serve as alternatives. That points to another problem with both the Mercantilist and PTT models: it encourages tendencies for the local delegee or government to restrict competition from global or external TLDs, as such restrictions might help them increase monopoly rents and/or the amount of control the national government exerts over local Internet users.

Pure sovereignty would also pose greater risks for the global compatibility of the DNS. A supranational authority such as the IANA would no longer be in a position to revoke or redelegate based on technical problems caused by a delegee. A subtler but in some ways longer term issue related to ccTLD sovereignty is the question: what will count as the sovereign part of the name space? Do only ISO-3166 codes count? Or could *any* names and International Domain Names that reference country names or geographic regions also be considered subject to sovereign rights? If the latter, the number of top-level domain names subject to sovereignty claims could become very large. Indeed, the success of states in asserting a linkage between sovereign control and a semantic reference seems to have already led to claims of governmental control over very broad categories of names: country names, names of geographic regions, acronyms of international organizations, etc. For example مصر, which is the name of the country 'Egypt' in Arabic script, was delegated by ICANN to the Egyptian National Telecommunication Regulatory Authority.[135] Palestine's government was also delegated its name in Arabic script.[136] Some countries assert sovereignty over registration of second level domain names that relates to the name of cities. For example IRNIC only allows the "respective administrative units" to apply for the name of the cities.[137] It is likely that such states would also assert sovereignty over the name of the cities at the top-level.

---

135. ICANN Resolutions, *Delegation of Egypt IDN ccTLD* (2010), https://features.icann.org/2010-04-22-delegation-egypt-idn-cctld.

136. Delegation of فلسطين. ("Falasteen") representing the Occupied Palestinian Territory in Arabic (2010), https://www.iana.org/domains/root/db/xn–ygbi2ammx.html.

137. NIC.IR, *Restricted Iran-Related Names*, http://www.nic.ir/Restricted_Iran-Related_Names.

In the recently concluded round of adding hundreds of new top-level domains, the GAC pushed for reservations of geographic names in all of them. The successful attempt by some Latin American countries to prevent a private company (Amazon) from registering its lawfully recognized trademark as a top-level domain is a sobering example of this phenomenon.[138] This tendency threatens to curtail freedom of expression and freedom of commerce, not only in the domain name space but on the Internet as a whole.

If sovereignty is not recognized in ccTLD delegation, then the model could go towards the property rights-based, Free Trade model, or the RFC 1591 global public trustee model.

B. Global Public Trustee

Due to its early problems with legitimacy, ICANN has backed away from Postel's and ICP-1's original global public trustee concept. As noted in our empirical analysis, ICANN does little to independently assess the level of stakeholder support in countries seeking a redelegation, and what little evidence it collects is used to confirm what the authorities want rather than to challenge or negate it. Insofar as ICANN has a role in delegations or redelegations, it has been confined to an interest in technical compatibility. However, it is not impossible for ICANN to take a stronger role in ccTLD delegations, as it already has done in gTLD delegations. Indeed, in the Iran case, ICANN reasserted the public trustee concept to support its claim that there are no property rights in a ccTLD string.[139] It is worthwhile to assess the merits and demerits of a stronger global public trustee model.

The advantages of making ICANN the administrator of the global public trust is that the Internet does constitute a globalized public sphere, or a community constituted through communication. A key part of the obligations of any ccTLD operator is to safeguard a local community's connectivity and compatibility with the rest of the world's Internet users. More ambitiously, an active, independent and honest global trustee administrator would be in a position to ascertain the views of the

---

138. GAC Early Warning (Nov. 20, 2012), https://gacweb.icann.org/display/gacweb/GAC+Early+Warnings?preview=/27131927/27197938/Amazon-BR-PE-58086.pdf.

139. Motion to Quash Writ of Attachment, *supra* note 17 ("As stated in ICANN's ccTLD guidelines, Section 9.1.3, 'the ccTLD is operated in trust in the public interest and that any claim of intellectual property rights in the two-letter code in itself shall not impede any possible future change of Registry.'").

various stakeholders in a country, independently of local power structures, and impose standards regarding good service and policy, using the global public interest as a standard. A global administrator would also be in a position to bypass dysfunctional or corrupt local delegees by redelegating to better operators. In failed or authoritarian states, or states lacking the infrastructure needed to provide good service it could even delegate the ccTLD to an operator outside the jurisdiction of the state in order to improve the service received by users of the domain. Such an approach would require a major expansion of ICANN/IANA's institutional capacity, however. It would have to be engaged in monitoring the performance of many delegees, which is costly. Such a path would also significantly increase ICANN's legal exposure, as it would be bestowing or removing valuable assets from local actors. It is already in a position to do so for gTLDs, although it tends to treat gTLD assignments more like property rights subject to "presumptive renewal."[140]

This option would constitute a significant power shift away from states and towards a transnational institution. This would be strongly resisted by national governments, although they would retain the ability to regulate local users and the ccTLD registry if it was located in its jurisdiction. It would also constitute an increase in the power of ICANN relative to incumbent ccTLD operators. It was evident from the reaction to ICP-1 that ccTLD registry operators view with alarm an ICANN empowered to review their performance and assess independently their accountability and support in their local communities. Thus, incumbent ccTLD operators, whether state-owned or private actor, would likely oppose a strengthened global public trustee model anchored in ICANN.

The flip side of the ability of a global trustee administrator to be independent of local power structures is that it might also become arbitrary or abusive, willing to put its own interests ahead of local preferences and needs in the selection of a delegee. Actors competing for valuable delegations would gravitate to ICANN to seek its blessing in their quest to take over a domain. ICANN

140. Section 4.2 of ICANN's base registry agreement contract provides for presumptive renewal, which implies that unless there is a material breach by the registry operator, or they themselves decide to sell their rights over the domain name, their agreement with ICANN will automatically be renewed after a certain term. Registry Agreement, ICANN, § 4.2 (Jan. 9, 2014), http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.pdf.

might also be too remote from the local community and not understand its needs as well as local actors. The accountability mechanisms to which ICANN is subject, both in the State of California and in its own bylaws and governance structures, would become much more important in such a regime. Also, given the robust global market for domain name registrations in hundreds of gTLDs as well as ccTLDs, and the possibility of local regulation, it is unclear why a trustee is needed to supervise TLDs.

C. Free Trade

The last option, Free Trade, would assign firmer property rights to ccTLD delegees and not recognize a role for sovereignty in delegation. Delegations would come from two basic sources: 1) the original delegations made by Postel and later by ICANN, and 2) voluntary transfers of the delegation, either by market transactions or by mutual agreement. Neither ICANN nor the state would have the ability to dictate a change in the delegee, though presumably a delegation, like any other form of property, could be lost due to criminal behavior or civil liability. The free trade model conceives of ccTLDs as registry services in a global marketplace, and would not require delegations to have any special obligations to the nation, residency or location requirements in the referenced territory.

A potential drawback of this model, in the minds of some, is that the ccTLD would no longer be a putative expression of national identity or national policy but more like an ordinary service provided in a global competitive market. The so-called 'quasi-generic' ccTLDs such as .IO (for British Indian Ocean Territory),[141] .CC (for the Cocos and Keeling Islands), .TV (for the island Tuvalu), and .ME come to mind as extreme examples of treating ccTLDs as assets detached from their original territorial reference. But the free trade approach does not *require* or even *encourage* ccTLD operators to turn away from their national

141. The Senior Minister of State, Department of Communities and Local Government & Foreign and Commonwealth Office testified that "the .io domain has always been carried out by a private sector organisation – this is currently the Internet Computer Bureau. As with the .uk domain, the Government receives no revenues from the sales or administration of this domain, and there are therefore no plans to share these with Chagossians." British Indian Ocean Territory Question Asked by Lord Avebury, Lord Avebury, UK Parliament House of Lords, July 10, 2014, http://www.publications.parliament.uk/pa/ld201415/ldhansrd/text/140710w0001.htm.

market or identity. Many if not most ccTLD delegees would continue to focus on their country market, as that is where they have established share and where the semantics of their TLD name gives them a competitive advantage. There is room for nonprofit and cooperative business models, just as there is room for noncommercial activity in any other part of a market economy. InternetNZ (.NZ) and the German ccTLD operator DENIC (.DE), for example, could be considered exemplars of the Free Trade category. Although they are organized as nonprofit cooperatives, they are run by private foundations and received their original delegations neither from ICANN nor from their government. Both are extremely protective of the security and autonomy of their delegation, viewing it as a valuable asset that belongs to the corporation rather than as a contingent trust granted to them by ICANN or a public authority. Both focus primarily on their national market, though tend to have liberal policies regarding registration by people outside the territory.

The Free Trade model neatly resolves the slippery slope problem created by making semantic references a basis for sovereignty claims. It eliminates the distinction between generic and territorial names. Governments would have no special authority over the delegation of ccTLD names. Incumbent ccTLDs would have the best of both worlds: a recognized right to their delegation without the same kind of contractual regulation by ICANN as gTLDs. It is important to add that nothing about holding the delegation as a property right exempts the delegee from normal forms of business regulation within its jurisdiction. If, for example, a national regulatory authority determined that a ccTLD registry was dominating the local market for domain name registration using illegal methods of competition, it could invoke remedies from competition law. The difference is that this model does not let the local government control to whom it is delegated, nor impose public trustee obligations on the delegee.

Based on some of the cases brought before courts, one might fear that a property rights based model would lead to instability by facilitating litigation to confiscate domains. This fear is, we think, unfounded. As noted in our legal analysis in section 5, there are limits on attachment, especially across jurisdictions. These limitations include consideration of third party impairments. The most extreme confiscation case, in which the State of Kentucky tried to seize the (second-level) domain names of gambling sites, was a bald attempt to assert extra-territorial jurisdiction and

foundered on that basis.[142] Even though domains can be considered property, the registry operators who hold the domains are located in specific jurisdictions and need only respond to lawsuits that create colorable claims in those jurisdictions. As noted before, there are statutory obstacles to attempts to apply garnishment claims to service contracts. And if ICANN was not legally responsible for the award of the property right (as it would be if it were the administrator of a global public trustee arrangement), ICANN would be less susceptible to litigation to take away the right. This model does not prevent repressive governments from controlling local ccTLD registries, especially if such governments already hold the delegation. But it does make it more difficult for them to change delegations at their whim.

6. SUMMARY AND CONCLUSIONS

Internet governance creates a complex mixture of legal and institutional arrangements. There is a strong interest in global technical compatibility, which necessitates governance arrangements that transcend national boundaries. There are also important economic interests in trade and investment across boundaries. States have a legitimate regulatory interest in the operation of the domain name market and other Internet services in their territory, but their jurisdiction must necessarily be limited to their own territory.

This paper was the first to subject sovereignty claims over ccTLD delegations to critical scrutiny. We can summarize its conclusions on that topic as follows: Is control of a ccTLD delegation a requirement of state sovereignty? No. Does the fact that ccTLD strings semantically refer to states mean that states have sovereignty rights over their delegation? No. Have states nevertheless succeeded in exploiting the isomorphism between the ISO-3166 codes and political geography to successfully assert more authority over ccTLD delegations than they originally had? Yes, and their agenda was strongly aided by the preeminent position of one sovereign, the United States, in the ICANN regime. Do states have a plausible, sovereignty-based claim to be able to regulate a domain name registry located in their territory? Yes, just as they can plausibly claim sovereignty over *any* business located and operating within their territory—but this claim to sovereign control is based on traditional forms of jurisdictional nexus and has

142. Commonwealth of Kentucky v. 141 Internet Domain Names, No 08-CI-1409 2008 WL 5261775 (Ky. Cir. Ct. 2008).

nothing to do with the fact that the ccTLD string contains a semantic reference to the country.

Ultimately, sovereignty has limited value as the basic principle for global governance of the domain name system and ccTLD delegations. As a globally shared resource, the DNS root needs to be unimpeded by sovereign claims, just like the high seas or outer space. The fact that ccTLDs are not major authority structures within a country but simply one DNS registry service among hundreds of others means that they operate in a globally competitive market. New TLDs can always be created. There is, therefore, little justification for linking state sovereignty to the delegation of a TLD. Governments can still use their sovereign powers to regulate the business practices of ccTLDs—and the Internet generally—if needed, with the caveat that this power can be, and routinely is, abused to engage in protectionism, expropriation and the suppression of free speech. Subjecting delegations to sovereignty claims simply amplifies the potential for arbitrary and politicized interventions in the Internet, while adding little value.

This paper has shown that ccTLD registrations have all the economic characteristics of a tradable property right: use, control, exclusivity, transferability. While domain name registries, in addition to supplying the name itself, provide a service to users that make domains operational, the possession of a unique top-level name registration is an essential input into the provision of a registry service, and the registry's customers must also possess a unique name registration. Many court decisions in various jurisdictions have recognized domains as property, even when they stop short of legally deciding that issue. The only court decision that claimed to rule that a domain was a service and not property, *Lockheed*, was based on a misunderstanding of the workings of the domain name system. The most vocal opponents of recognizing property rights in domains are typically registries higher up in the domain hierarchy, who see property rights in lower levels of the naming hierarchy as a threat to their own property right at a higher level of the naming hierarchy. Finally, we have shown that most court decisions denying a plaintiff's right to attach or seize a domain are based on factors other than the property status of the domain. Most notably, the appeals court decision in *Weinstein* was based on a concern about the way a court-ordered property transfer might impair the interests of third parties, particularly ICANN and second-level domain name registrants.

Regarding its implications for ICANN, our analysis supports ICANN as the administrator of a global public trustee regime, but its criteria for recognizing and implementing delegations must be very narrowly limited to its interest in the *global compatibility of the DNS*. That is, the public benefit for which it serves as the steward is limited to the technical coordination and compatibility function at the root. ICANN should not be involved in determining who is the "best" delegee for a territory, nor should it be involved in using its leverage over delegations to regulate the prices, practices or policies of ccTLDs except insofar as its practices affect its compatibility with the global DNS.

In line with this conclusion, the paper's assessment of the four governance models indicates that the Free Trade model, supplemented by a narrowly construed public trustee ICANN regime focused on technical compatibility, seems to have the most desirable characteristics. Recognizing property rights in delegations paves the way for a more stable and open global market in domain name registry services by providing an orderly mechanism for redelegations subject to important forms of market discipline.