A *Stern* Look at the Property Status of Top-Level Domains

William Larsen†

INTRODUCTION

Top-level domains (TLDs) are the right-most portion of a web address.[1] For example, in "web.address.com," ".com" is the TLD. TLDs are divided into generic TLDs (gTLDs), such as ".com" and ".net," and country-code TLDs (ccTLDs), such as ".us," ".uk," and ".ca."[2] Broadly speaking, gTLDs are administered by private entities through agreements with the Internet Corporation for Assigned Names and Numbers (ICANN), a US-based nonprofit corporation.[3] ccTLDs, in contrast, are administered either by the government associated with a particular ccTLD or by a designated private entity.[4]

Despite the importance of the domain name system (DNS) to the Internet, the legal status of TLDs is uncertain. Few cases have addressed the related legal issues; courts have not arrived at a consensus regarding either the property status of TLDs or, if TLDs are property, who actually owns a given TLD.[5] Some

---

† BA 2011, The University of Chicago; JD Candidate 2016, The University of Chicago Law School.

1 See Jon Postel, *Domain Name System Structure and Delegation* *1 (Internet Engineering Task Force Network Working Group, Mar 1994) ("RFC 1591"), archived at http://perma.cc/6HND-9UYN.

2 See Internet Assigned Numbers Authority, *Root Zone Database*, archived at http://perma.cc/VM28-Q3XJ. The Internet Corporation for Assigned Names and Numbers (ICANN) distinguishes between two gTLD subtypes—unsponsored gTLDs (uTLDs) and sponsored gTLDs (sTLDs)—based on whether the gTLD is intended to be used by a wide community or narrow subcommunity, respectively. For more information on the distinction between unsponsored and sponsored gTLDs, see Internet Corporation for Assigned Names and Numbers, *Top-Level Domains (gTLDs)*, archived at http://perma.cc/62HH-9MFE. ICANN also recognizes one infrastructure TLD: ".arpa." See IANA, *Root Zone Database* (cited in note 2).

3 See Torsten Bettinger, ed, *Domain Name Law and Practice: An International Handbook* 22–23 (Oxford 2005).

4 See id at 5.

5 See, for example, *Stern v Islamic Republic of Iran*, 2014 WL 5858095, *3 (DDC 2014) (noting that "[t]here is little authority" on whether domain names may be attached in satisfaction of a judgment).

TLDs are eligible for trademark protection, while others are not.[6] Some TLDs can be alienated by their administrators, while others cannot.[7] Some TLDs can restrict registration of subdomains, while others cannot.[8] With regard to the DNS more generally, some domains may be seized to satisfy claims or debts, while others may not.[9]

This Comment attempts to unify case law, statutory law, and extralegal norms into an overarching theory explaining the property status of TLDs. Because transactions relating to TLDs take place both inside and outside of formal legal frameworks, an assessment of TLDs' property status must account for both legal decisions relating to the DNS and extralegal events that illuminate a community consensus on which property rights should be recognized in TLDs.[10]

Part I explains the technical background of the DNS and provides a brief historical overview of major events implicating TLD ownership. Part II considers cases and statutes relating to domain names and TLDs and identifies two strains of judicial interpretation. Specifically, courts have generally followed either an abstract-property theory or a service theory in deciding whether a given domain name is subject to transfer. Part III attempts to reconcile this case law with extralegal practice, arguing for an approach to TLDs that weighs four normative considerations: stability, predictability, descriptive accuracy, and respect for the interests of the Internet community at large. Ultimately, the best solution is to view TLDs as analogous to Federal Communications Commission (FCC) wireless-spectrum licenses: TLD operators exercise some private rights while ICANN retains the public right to regulate TLD policy. Viewing TLDs as licenses balances the normative interests and provides an established body of law for formal adjudication of TLD disputes.

---

6 See Part II.A.1.

7 See Part II.A.3.

8 See Part II.B.2.

9 See Part II.A.2.

10 For a discussion of the interaction between legal and extralegal standards in cyberlaw, see generally Bruce L. Benson, *The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement without the State*, 1 J L Econ & Pol 269 (2005).

I. BACKGROUND AND TECHNICAL OVERVIEW

Courts have not always grasped how domain names and TLDs operate. As this Comment argues, one major failing in TLD doctrine has been a lack of descriptive accuracy—in other words, a mismatch between how legal doctrines describe TLDs and how TLDs actually work. Addressing this issue requires an understanding of the technical systems that underlie the DNS. This Part first discusses the relevant aspects of the DNS's technical side. Then, to clarify the current organization of rights and responsibilities relating to TLD management, this Part provides a brief overview of the DNS's historical development.

A. The Internet DNS

Every website is located at an Internet-protocol (IP) address—a long string of numbers that looks like "192.168.0.1".[11] Because these numbers tend to be difficult to memorize, the DNS translates between numerical IP addresses and their corresponding plain-text web addresses. The DNS distinguishes between TLDs (such as ".com" or ".au") and subdomains (a domain that is part of a larger domain). Because each IP address can correspond to only a single domain name, only one party can provide the instructions that redirect an end user to a website when the end user enters a particular domain name.[12] In other words, for the DNS to work, there can be only one "google.com" and only one master list of which subdomains are registered under ".com."

When a network device like a computer or cell phone wishes to connect to a website—say, "calendar.google.com"—it makes a

---

[11] This particular IP address is reserved for local addresses. Popular websites utilize multiple IP addresses to handle the enormous amount of traffic they receive. Google, for example, uses the IP ranges 63.233.160.0 to 64.233.191.255, 74.125.0.0 to 74.125.255.255, and 209.85.128.0 to 209.85.255.255, among others. The above are examples of IPv4 addresses; the newer IPv6 addresses look like "2001:0cb8:85a4:0000:0000:8a3d:0460:7342"; they amply demonstrate why coordination through the DNS is necessary. See Robert M. Hinden and Stephen E. Deering, *IP Version 6 Addressing Architecture* *3–5 (Internet Engineering Task Force, Network Working Group, July 1998), archived at http://perma.cc/4DX5-BCPB.

[12] See P. Mockapetris, *Domain Names - Implementation and Specification* (Internet Engineering Task Force Network Working Group, Nov 1987), archived at http://perma.cc/L22X-7U9F. See also Internet Corporation for Assigned Names and Numbers, *Beginner's Guide to Domain Names* *3 (Dec 2010), archived at http://perma.cc/J7MM-DVT8.

multistep query.[13] First, the device must figure out where ".com" is located; to answer this question, it needs to ask the root name server. The root name server is a server (or, more accurately, a system of servers) containing the definitive listing of the location of every TLD within the DNS.[14] Once the device learns from the root name server where ".com" is located, it asks the ".com" servers where "google.com" is located. Finally, when the device knows where "google.com" is located, it asks the "google.com" servers where "calendar.google.com" is located.[15] While this process is quite fast, it is actually the result of many servers in geographically distant locations operating sequentially.[16] Importantly, a TLD without a subdomain listed does not resolve into an IP address—trying to visit ".com" is impossible.

If the root name servers disagree on how to resolve a particular query, the Internet may become fractured and requests for a particular domain may return different results depending on which network the requesting device is connected to. For example, Internet users in Kansas might see a different "google.com" than Internet users in Cancun—and, potentially, only one of these might be Google's desired "google.com." Users of different networks may still be able to communicate through other methods—for example, through Twitter or an e-mail protocol—but they will not be able to visit conflicting webpages on the other network. This is known as "splitting the root," and commentators consider this a disastrous outcome for the future of

---

[13] For an overview of this process, see A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution*, 50 Duke L J 17, 37–42 (2000).

[14] While this is how the DNS is structured, DNS resolution often works differently in practice. Web-enabled devices have caches that store the addresses of popular websites and name servers, enabling requests to be resolved more quickly. See Daniel Karrenberg, *DNS Root Name Servers Frequently Asked Questions* (Internet Society, Feb 2008), archived at http://perma.cc/3UTR-CGWK. For a more detailed explanation, see Roy Fielding, Mark Nottingham, and Julian Reschke, *Hypertext Transfer Protocol (HTTP/1.1); Caching* *4–6 (Internet Engineering Task Force, June 2014), archived at http://perma.cc/N29W-MBD4.

[15] The part of the domain name listed as "calendar" in this example is known as a host name or leaf domain. See P. Mockapetris, *Domain Names - Concepts and Facilities* *6–7 (Internet Engineering Task Force Network Working Group, Nov 1987), archived at http://perma.cc/7V2J-PCJ3.

[16] See Froomkin, 50 Duke L J at 21 n 7, 42–43 (cited in note 13). Some private entities operate alternate DNS processes. For example, Google operates its own DNS servers. See *Public DNS* (Google Developers, Mar 31, 2015), archived at http://perma.cc/TD8P-PKY5. Networks that block sites—for example, airline wireless networks that prohibit streaming services—sometimes do so by redirecting DNS queries away from their intended targets to certain specified sites.

the Internet: if the Internet's great success is due at least in part to the free and unimpeded flow of information across people, distances, and devices, a fractured web threatens this freedom by separating users of different networks.[17] Splitting the root also creates a serious externality problem for domain name owners, whereas maintaining a single, unified root ensures that any given domain name is accessible on any device in the world.[18]

The root name servers remain unified by syncing to a file called the root zone file, which contains the master list of every TLD's location within the DNS.[19] There are currently thirteen root name servers, named A through M.[20] Until 1987, however, there were only four, all of which were located in the United States; when the DNS was expanded to increase general performance and decrease system load,[21] the number of stateside servers grew to ten, and three additional servers were introduced outside the United States.[22] Now, the root name servers are decentralized among hundreds of physical server instances but remain grouped within the A through M designations.[23] The crucial aspect of the DNS for property purposes is that each name server synchronizes its root zone file with the A name server—a synchronization that is vitally important to ensure a unified root. The A name server is currently operated by Verisign under contract with the US government.[24] The

---

17 See Wolfgang Kleinwächter, *De-mystification of the Internet Root: Do We Need Governmental Oversight?*, in William J. Drake, ed, *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* 209, 224 (United Nations 2008):

> The negative consequences of such fragmentation would be the end of the ubiquity of the Internet in which everywhere everybody could communicate every time with everybody. A system with diversified roots . . . would reduce Internet freedoms, choices and options . . . and would make it much easier for restrictive Governments to control the virtual life of their citizens.

18 See Markus Müller, *Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet*, 15 Fordham Intel Prop, Media & Enter L J 709, 716 (2005). See also Milton L. Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction?* *2–3 (Oct 2001), archived at http://perma.cc/TJM4-BRTU.

19 See Mueller, *Competing DNS Roots* at *3 (cited in note 18).

20 See *Root-servers.org*, archived at http://perma.cc/E6E6-WSXG.

21 Before 1987, mappings of host names to addresses were contained in a single text file (hosts.txt). This resulted in significant bandwidth usage. See Mockapetris, *Domain Names* at *1–2 (cited in note 15).

22 See Harold Feld, *Structured to Fail: ICANN and the "Privatization" Experiment*, in Adam Thierer and Clyde Wayne Crews Jr, eds, *Who Rules the Net? Internet Governance and Jurisdiction* 333, 337 (Cato 2003). See also *Root-servers.org* (cited in note 20).

23 See *Root-servers.org* (cited in note 20).

24 See *A.root-services.net* (Verisign), archived at http://perma.cc/HE4Q-3T4H.

operators of the B through M name servers work outside of the direct control of any higher organization but nevertheless acknowledge their responsibilities through agreements with the Internet Assigned Numbers Authority (IANA) and ICANN.[25]

Ownership of the root zone file is a high-stakes question.[26] Whoever controls the root zone file can add or remove TLDs within minutes and can designate the registry operator for each TLD.[27] Registration of subdomains generates millions of dollars in revenue for the registrars each year, and a collection of subdomains under popular TLDs contains significant intellectual property interests.[28] Similarly, administration of TLDs can carry significant policy implications: lax administrators provide a haven for malware sites, digital piracy, or trademark infringement.[29] Although TLD ownership has rarely been contested in US courts, the underlying property interests are valuable not just for the registration revenue and intellectual property interests they impact but also for the multibillion-dollar e-commerce industry they support.

---

[25] See Internet Corporation for Assigned Names and Numbers, *Model MoU for Root Nameserver Operations* (Jan 21, 2002), archived at http://perma.cc/N5JR-7X3K. See also Karrenberg, *DNS Root Name Servers Frequently Asked Questions* (cited in note 14).

[26] See Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* 30–32 (Oxford 2006) ("Not only does the domain name system affect valuable Internet-related property rights, it also has the potential to serve as a powerful tool of Internet enforcement and to shape the nature of the Internet itself.").

[27] A registry operator administers the zone file for a given TLD (sometimes referred to as "the registry"), entering second-level domains as requested by registrars. See Internet Corporation for Assigned Names and Numbers, *Glossary* at "Registry", archived at http://perma.cc/6X3M-55VT. As a result, a registry operator is ultimately responsible for the addition or removal of a given subdomain and can change the operator of a given subdomain as requested. See Internet Corporation for Assigned Names and Numbers, *FAQ for Name Reservation, Allocation, and Reservation* *1 (Aug 8, 2014), archived at http://perma.cc/Q2Y3-GA4G. In practice, this addition and deletion can be managed by accredited registrars, which are generally independent entities under contract with ICANN. Sometimes, however, the registry operator may serve as a registrar as well. See Internet Corporation for Assigned Names and Numbers, *Information for Registrars and Registrants*, archived at http://perma.cc/SAC2-HAGU.

[28] For a discussion of the complexities surrounding virtual-property interests, see generally David Nelmark, *Virtual Property: The Challenges of Regulating Intangible, Exclusionary Property Interests Such as Domain Names*, 3 Nw J Tech & Intel Prop 1 (2004).

[29] See Leigh Metcalf, *A ccTLD Case Study: .tv* (Carnegie Mellon University, July 12, 2013), archived at http://perma.cc/6SRD-69SD.

B. History of De Facto Ownership over the DNS

The Internet domain name system was originally designed and operated by Jon Postel.[30] Postel proposed and implemented many of the earliest gTLDs, such as ".com," ".edu," and ".net."[31] By 1988, Postel's authority over the DNS was made official through a contract between the Department of Defense (DOD) and the Stanford Research Institute.[32] While much early Internet research was funded by the DOD and the National Science Foundation in conjunction with research universities, the US government was largely content to leave administrative policy determinations (such as the organization and specification of the DNS) to those with technical expertise; Postel's arrangement was no exception.[33] This contract also founded the IANA, which was originally responsible for the allocation of the unique names and numbers used by the DNS. This function—assigning blocks of unique IP addresses to Regional Internet Registries (RIRs) and administering the root name servers—is known as the "IANA function."[34]

In 1990, as the result of defense-contract regulation, root zone control—that is, control over the A name server, to which the other root name servers synced the root zone file containing the master list of TLDs—was transferred from the Stanford Research Institute to Network Solutions, Inc (NSI).[35] This transfer sparked the first major battle for control of the DNS. The Internet technical community, consisting mostly of the engineers and computer scientists who created the web's infrastructure, generally believed that the DNS should rest in the hands of a nonprofit, nongovernmental entity serving the larger Internet community.[36] In their view, the Internet's growth from a limited network among US-based research universities to a global phenomenon necessitated a governing structure more responsive to international concerns and less swayed by US-specific

---

30 Postel retains mythical status among Internet historians for administering the DNS in the early stages of the Internet and for serving as the primary manager of the IANA function until his death in 1998, among other significant contributions. See Goldsmith and Wu, *Who Controls the Internet?* at 33–36 (cited in note 26).

31 See id at 33.

32 See id at 35.

33 See id at 33.

34 See Internet Corporation for Assigned Names and Numbers, *IANA Functions: The Basics*, archived at http://perma.cc/P52D-GPPX.

35 See Goldsmith and Wu, *Who Controls the Internet?* at 35 (cited in note 26).

36 See id at 35–38.

interests—interests that community members believed were already jeopardizing the Internet's future growth, as evidenced by NSI's handling of registry responsibilities.[37] In 1997, these community members formed the Internet Ad Hoc Committee (IAHC) and published a quasi manifesto known as the Generic Top-Level Domain Memorandum of Understanding, outlining plans to establish an independent governing group in Switzerland for the DNS and the IANA function.[38]

While many in the Internet community supported the IAHC's efforts, the US government took a different view. Much of the early Internet infrastructure was developed as a result of collaboration among research universities, the DOD, and the National Science Foundation.[39] As such, the US government believed that it was ultimately best positioned to shepherd the Internet's growth, balancing the competing pressures of "predictability and security" on the one hand and freedom from "micro-regulations" on the other; for these reasons, the US government asserted that the DNS and the root zone file belonged under US control.[40] The United States' position was motivated both by skepticism about the accountability of a privately held Internet and by a desire to ensure the Internet's responsiveness to the interests of "the U.S. government, [ ] foreign governments, [and] business."[41]

As a challenge to US authority over the DNS, Postel directed name servers not under NSI control to synchronize with his B name server instead of NSI's A name server.[42] NSI still maintained authority over the A name server, but, for a brief period, eight of the other name servers synced their copies of the

---

[37] See Heather N. Mewes, *Memorandum of Understanding on the Generic Top-Level Domain Name Space of the Internet Domain Name System*, 13 Berkeley Tech L J 235, 238–39 (1998).

[38] The Internet Community, *Establishment of a Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System (gTLD-MoU)* (International Telecommunication Union, Feb 28, 1997), archived at http://perma.cc/MW2N-S4TD.

[39] See Scott J. Shackelford and Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 Stan J Intl L 119, 125–26 (2014).

[40] Goldsmith and Wu, *Who Controls the Internet?* at 40–43 (cited in note 26) (quotation marks omitted).

[41] Id at 42.

[42] Id at 43–46. The actual legal status of Postel's move was questionable, but as Postel was the father of the system, the name-server operators deferred to him. As one name-server operator described: "If Jon asks us . . . we'll do it. He is the authority here." Id at 44.

root zone file with Postel's B name server instead.[43] Postel's move threatened to split the root: if he had decided to change anything in the root zone file, users connected to the nine name servers under his control would see different DNS-query results than users connected to the three name servers that remained with NSI. The move was more symbolic than threatening, given that Postel's B name server continued to sync with NSI's A name server. But the implications were clear. The Clinton administration threatened Postel, demanding that he reverse the changes and resume synchronizing the name servers with NSI's root zone file on the A name server.[44] Postel complied. The US government had successfully claimed control of the DNS.[45]

The US government's move was not viewed favorably in the Internet technical community. Misgivings about DNS control resting in government hands were widespread; furthermore, the United States' designated administrator, NSI, drew heavy criticism for abusing its artificial monopoly to the detriment of the Internet community.[46] In response to these criticisms and to an antitrust suit from a would-be competing TLD registrar,[47] the United States proposed to privatize the IANA function by transferring DNS control to an independent nonprofit to be incorporated under US law and involving international participation.[48] Despite concerns, the privatization

---

[43] See id at 44–45. At this time, the name-server operators operated voluntarily and could thus make these changes without running afoul of any contractual obligations. Today, name-server operators recognize an obligation to provide this service. See Karrenberg, *DNS Root Name Servers Frequently Asked Questions* (cited in note 14).

[44] See Goldsmith and Wu, *Who Controls the Internet?* at 45–46 (cited in note 26).

[45] See id.

[46] See Feld, *Structured to Fail* at 341–42 (cited in note 22). NSI was the first beneficiary of the US government's attempt to privatize DNS functions. For a detailed history of NSI's role and the criticisms of its management of the DNS, see Daniel J. Paré, *Internet Governance in Transition: Who Is the Master of This Domain?* 19–23 (Rowman & Littlefield 2002).

[47] See *PGMedia, Inc v Network Solutions, Inc*, 51 F Supp 2d 389, 395 (SDNY 1999) (alleging antitrust violations against NSI as the sole provider of Internet domain name registration services).

[48] See Improvement of Technical Management of Internet Names and Addresses, 63 Fed Reg 8826, 8827–28 (1998) ("We propose the creation of a private, not-for-profit corporation (the new corporation) to manage the coordinated functions in a stable and open institutional framework. The new corporation should operate as a private entity for the benefit of the Internet as a whole.").

proposal was finalized in 1998,[49] and within months ICANN was formed.[50]

The US government[51] agreed to transfer administration of the DNS and the IANA function to ICANN shortly thereafter.[52] ICANN manages both the technical and policy components of the DNS today.[53] ICANN does not actually own the root zone file; any changes to TLD registrars or the addition or deletion of any TLDs must instead be approved by the Department of Commerce.[54] However, the Department of Commerce does not initiate changes to the root zone file and generally does not deny any changes requested by ICANN.[55]

Two recent developments are important to resolving the question whether TLDs manifest property rights. First, ICANN has added more than one hundred new TLDs within the last decade.[56] These additions fall into two broad categories. The first category contains non-Latin ccTLDs for countries like Russia, Saudi Arabia, and Japan to resolve Cyrillic, Arabic, and other non-Latin domain names into IP addresses.[57] The other category includes sponsored gTLDs, which are operated by private entities under contract with ICANN, including such new TLDs as

---

49 See Management of Internet Names and Addresses, 63 Fed Reg 31741, 31751 (1998) ("White Paper").

50 IANA is now a department within ICANN. See Internet Assigned Names Authority, *Introducing IANA*, archived at http://perma.cc/SWG9-GUM3.

51 While early Internet research was conducted through contracts between the DOD, the National Science Foundation, and research universities, by the late 1990s the Department of Commerce's National Telecommunication and Information Administration (NTIA) took over primary responsibility for DNS regulatory issues. See National Research Council, *Signposts in Cyberspace: The Domain Name System and Internet Navigation* 76–77 (National Academies 2005).

52 See *Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers* (Nov 25, 1998), archived at http://perma.cc/76K4-WXMW.

53 See Internet Corporation for Assigned Names and Numbers, *What Does ICANN Do?*, archived at http://perma.cc/4GWH-8JQE.

54 See Cyrus Farivar, *ICANN to Plaintiffs: No, You Can't Have All of Iran's Domains* (Ars Technica, July 30, 2014), archived at http://perma.cc/86W6-PN7Q.

55 See Feld, *Structured to Fail* at 347 (cited in note 22). One notable exception is the ".xxx" domain debacle, in which the US government was accused of interfering in ICANN negotiations with ICM, the prospective ".xxx" gTLD registry operator. See, for example, Scott P. Sonbuchner, Note, *Master of Your Domain: Should the U.S. Government Maintain Control over the Internet's Root?*, 17 Minn J Intl L 183, 200 (2008).

56 See Internet Corporation for Assigned Names and Numbers, *Largest Domain Name Expansion in Internet's History Reaches Benchmark* (Jan 21, 2014), archived at http://perma.cc/L625-RGLT.

57 See Internet Corporation for Assigned Names and Numbers, *Internationalized Domain Names*, archived at http://perma.cc/8EDZ-AXTF.

".yachts," ".republican," and ".hamburg."[58] The second major development is that the Department of Commerce has announced that it plans to relinquish control over the root zone file.[59] ICANN is currently drafting a transfer proposal; it is not yet clear whether ICANN will propose to take over that controlling role itself.[60]

These two trends call the legal framework surrounding TLDs into question, and courts have begun to face more questions as to whether TLDs retain aspects of property. Some established legal postures—such as unquestioned US control over the DNS and the broad, generic character of the older gTLDs—no longer seem certain. Given the importance of a unified, stable DNS to a global economy that increasingly relies on the free exchange of information via the Internet, resolution of the legal entitlements involving TLDs has become critical.

II. TWO THEORIES OF TLDS: ABSTRACT PROPERTY OR SERVICE?

Courts have struggled when faced with the question whether a given domain name or TLD carries recognizable property rights. Different areas of law point in different directions. Trademark cases have long recognized intellectual property interests in subdomains and have recently indicated a willingness to grant the same to TLDs, but courts have not

---

[58] See Internet Corporation for Assigned Names and Numbers, *Delegated Strings* (2015), archived at http://perma.cc/9NBL-2BUK.

[59] See National Telecommunications and Information Administration, *NTIA Announces Intent to Transition Key Internet Domain Name Functions* (Mar 14, 2014), archived at http://perma.cc/GT22-BT28. However, Congress has attempted to block the NTIA from transitioning the IANA functions outside of US-government control. See Consolidated and Further Continuing Appropriations Act, 2015 § 540(a), Pub L No 113-235, 128 Stat 2130, 2217 (2014):

> None of the funds made available by this Act may be used to relinquish the responsibility of the National Telecommunications and Information Administration during fiscal year 2015 with respect to Internet domain name system functions, including responsibility with respect to the authoritative root zone file and the Internet Assigned Numbers Authority functions.

The NTIA, for its part, remains committed to the transition. See *Remarks by Assistant Secretary Strickling at the State of the Net Conference* (National Telecommunications and Information Administration, Jan 27, 2015), archived at http://perma.cc/3NZA-PDQU.

[60] The United States General Accounting Office has questioned whether the Department of Commerce can give away root zone control. See Robert P. Murphy, *Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers* *2 (United States General Accounting Office, July 7, 2000), archived at http://perma.cc/AD73-7YV5. See also Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* 197 (MIT 2002).

articulated a settled principle. Cases involving asset seizure—either in the context of tort cases, contractual liability, or civil forfeiture for criminal copyright violations—have taken divergent approaches. Finally, a recent case involving attachment of a ccTLD to satisfy tort liability points to an interesting but ultimately unsatisfactory solution.

Two distinctions must be made at the outset. The first is between subdomains and TLDs. Commentators and courts have sometimes neglected to recognize that these are separate concepts. Second, and similarly, ccTLDs and gTLDs operate in basically identical fashions but implicate different sets of concerns: ccTLDs raise questions of sovereignty and international law,[61] while gTLDs are more markedly commercial in nature.[62] Whether these distinctions call for recognition of correspondingly distinct legal rights is a separate question.

While remaining mindful of the differences between subdomains and TLDs, this Part examines case law, statutes, and extralegal events relevant to the question of TLDs' property status. There are two main trends moving in opposite directions. On the one hand, increasing recognition of property interests in subdomains—such as that which appears in trademark—is beginning to filter over to views on TLDs. On the other hand, comparisons of subdomains to nonproperty concepts like street addresses or telephone numbers have gained a foothold in the realm of bankruptcy and attachment. Neither the pro-property view nor the anti-property view can count a decisive victory yet, but each view garners substantial support from different facets of the law.

A. TLDs Recognized as Property

Over the past few years, US law has seen a "movement towards treating a domain name as simple property, susceptible to seizure and usable as a source of *in rem* jurisdiction."[63] This shift has taken place almost entirely with subdomains, rather

---

[61] See generally Kim G. von Arx and Gregory R. Hagen, *Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control*, 9 Richmond J L & Tech 4 (2002).

[62] See Joseph P. Smith III, *The Tangled Web: A Case against New Generic Top-Level Domains*, 20 Richmond J L & Tech 1, 14 (2014) (noting ICANN's justification for new gTLDs as a "business opportunity" for registrars) (quotation marks omitted).

[63] Jack Mellyn, *"Reach Out and Touch Someone": The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law*, 42 Georgetown J Intl L 1241, 1247 (2011).

than TLDs; only one case has raised the question whether a TLD can be seized.[64] Nevertheless, insights developed in the law of subdomains may prove useful for answering the question whether TLDs contain property rights. Subdomains and TLDs share significant technical similarities, despite the differences in their uses; legal doctrine that is applicable to one, then, may reflect principles relevant to the other. At the same time, given these differences, the wisest path may involve some separation between the two doctrines when the legal question more directly touches a unique aspect of subdomains or TLDs—for example, the fact that subdomains point an end user to a specific webpage, while TLDs are often more valuable as collections of registered subdomains. Subdomain cases, then, can be helpful, but they should be evaluated critically before being directly applied to the realm of TLDs. This Section identifies three theories in favor of a view of TLDs as property, some more heavily grounded in the law of subdomains than others.

1. Trademark protection for TLDs.

Courts have long recognized trademark protection in subdomains. In the early days of the Internet, cybersquatters registered trademarks of large corporations as web addresses and attempted to sell these domains back to the trademark owners at a premium; some companies paid the cybersquatters' bounties, while others brought actions against cybersquatters.[65] Two of the earliest decisions to address the question whether cybersquatters could face liability under the Lanham Act[66] for registering trademarks as webpages were decided in favor of trademark protection.[67] Later courts have followed suit.[68]

---

64 See *Stern v Islamic Republic of Iran*, 2014 WL 5858095, *3 (DDC 2014). See also Part II.B.2.

65 See P. Wayne Hale, Note, *The Anticybersquatting Consumer Protection Act & Sporty's Farm L.L.C. v. Sportsman's Market, Inc.*, 16 Berkeley Tech L J 205, 206–07 (2001).

66 Pub L No 79-489, 60 Stat 427 (1946), codified at 15 USC § 1051 et seq.

67 See *Panavision International, LP v Toeppen*, 141 F3d 1316, 1327 (9th Cir 1998); *Intermatic, Inc v Toeppen*, 947 F Supp 1227, 1241 (ND Ill 1996). Both of these cases were brought against the same cybersquatter defendant. See *Panavision International*, 141 F3d at 1318; *Intermatic*, 947 F Supp at 1228.

68 See, for example, *E & J Gallo Winery v Spider Webs Ltd*, 286 F3d 270, 277 (5th Cir 2002); *Sporty's Farm LLC v Sportsman's Market, Inc*, 202 F3d 489, 499 (2d Cir 2000). The adoption of the Anticybersquatting Consumer Protection Act (known as the ACPA and discussed at greater length in Part II.A.2) and the introduction of ICANN's arbitration procedures (known as the Uniform Domain-Name Dispute-Resolution Process, or UDRP) have introduced alternate routes for plaintiffs seeking protection against

Although trademark protection for subdomains is settled, a remaining question involves the extent to which subdomains have property characteristics independent of the intellectual property interests reflected therein. One way to resolve this is by looking toward remedies. The question of remedies remains open, and the types of remedies available largely depend on theories of the underlying property nature of domain names. Plaintiffs have sought a variety of remedies against both cybersquatters and others holding domain names that violate recognized trademarks.[69] For example, in *Brookfield Communications, Inc v West Coast Entertainment Corp*,[70] Brookfield sought and was granted an injunction that barred West Coast from using Brookfield's trademark in the domain name "moviebuff.com."[71] In other cases, plaintiffs have successfully forced the transfer of domain names from particularly egregious cybersquatters.[72] The fact that domain names may be transferable in cases of trademark violation is an important data point in answering the question of which property rights should be recognized in TLDs, and it implies a theory of domain names' property status that extends beyond trademark dilution.

Trademark protection did not traditionally extend to TLDs, but ICANN's expansion of the gTLD namespace has changed this picture. In *Image Online Design, Inc v Core Association*,[73] the plaintiff, Image Online Design, sought injunctive and monetary relief against a would-be competing registrar on the grounds that it held common-law trademark rights in the ".web" gTLD.[74] The ".web" gTLD was not in operation at the time,[75] but

---

cybersquatters. Additionally, as more plaintiffs opt for UDRP, litigation over cybersquatting appears to have decreased relative to UDRP claims. See Jordan A. Arnot, *Navigating Cybersquatting Enforcement in the Expanding Internet*, 13 John Marshall Rev Intel Prop L 321, 327 (2014).

69 Not all holders of domain names that violate trademarks do so in an attempt to cybersquat. See, for example, *Mattel v Barbie-Club.com*, 310 F3d 293, 299 (2d Cir 2002) (involving a lawsuit by Mattel alleging that an Australian barbeque company was diluting Mattel's trademarks by operating the "captainbarbie.com" subdomain).

70 174 F3d 1036 (9th Cir 1999).

71 Id at 1066–67.

72 See, for example, *Virtual Works, Inc v Volkswagen of America, Inc*, 238 F3d 264, 271 (4th Cir 2001). A transfer is authorized only if the plaintiffs succeed in proving their infringement claim under a heightened standard imposed by the ACPA. See 15 USC § 1125(d)(1)(a)(i) (requiring bad faith as a prerequisite for trademark liability under the ACPA). See also Part II.A.2 (discussing the ACPA in greater detail).

73 120 F Supp 2d 870 (CD Cal 2000).

74 Id at 872.

the defendant was selling ".web" subdomains to customers under the presumption that ICANN would eventually approve the ".web" gTLD. The court ruled against Image Online Design's claim on the grounds that ".web" was a generic mark that did not indicate source.[76] Because customers can obtain registration of a subdomain under many registrars, the Court reasoned, a particular TLD does not point to any one registrar as its "owner."[77] From this case, it initially appeared that both the extensive trademark protections applicable to subdomains—and with them, an implication of property—would not extend to TLDs.

However, a recent opinion by the Trademark Trial and Appeal Board (TTAB), an adjudicative body inside the United States Patent and Trademark Office (PTO), has recognized that after ICANN's decision to expand the TLD namespace, TLDs may serve a source-identifying function. In *In re theDot Communications Network LLC*,[78] the TTAB held that the ".music" gTLD was ineligible for trademark protection because it was "merely descriptive."[79] But importantly, the TTAB noted as an example in its decision that Canon, Inc planned to seek trademark protection for a potential ".canon" gTLD, and the TTAB indicated that ".canon" might be eligible for protection.[80] The implication of the TTAB's discussion is clear: certain sponsored gTLDs could be eligible for trademark protection if they meet the Lanham Act's requirements.[81]

At least one court has recognized the impact of the TTAB's dicta. In 2013, Image Online Design again attempted to gain recognition for its ".web" trademark—this time, by bringing an action against ICANN alleging that ICANN's plan to grant registry control of ".web" to competing applicants would violate Image Online Design's ".web" trademark and breach a contract

---

75 The ".web" TLD remains unused. See IANA, *Root Zone Database* (cited in note 2).

76 *Image Online Design*, 120 F Supp 2d at 876. By implication, this holding included all then-existing TLDs because the only TLDs existing at the time were those included in the original group of gTLDs designated by IANA plus the ccTLDs.

77 Id.

78 101 USPQ2d 1062 (TTAB 2011).

79 Id at 1068–69.

80 Id at 1067 n 22.

81 For these requirements, see 15 USC § 1052(e).

between Image Online Design and ICANN.[82] While the court again ruled against Image Online Design, it noted:

> [I]f ICANN were to introduce the TLD .APPLE, the user would arguably expect that that TLD is administered by Apple Inc. In such a case, the TLD might be considered a source indicator. If Sony tried to administer the TLD .APPLE, Apple Inc. would likely argue and possibly prevail on a trademark infringement claim.[83]

No case has subsequently arisen in which a plaintiff has successfully asserted trademark infringement against a TLD registry operator for its use of the TLD. But the expansion of the TLD namespace is very recent, and it might generally be expected that, given major brands' experiences with cybersquatters in the late 1990s and early 2000s, companies will register any potentially infringing TLDs.[84] Further, in 2013 the PTO took another step by initiating a change to its examination guide to allow for trademark protection of gTLDs.[85] The traditional position that TLDs cannot be trademarked has been called into question with the introduction of "brand" gTLDs like ".canon."

2. Operation in Our Sites and the Anticybersquatting Consumer Protection Act.

Mirroring the increasing trend in trademark law to recognize property protection for subdomains and TLDs, two federal statutory schemes support a view of domain names as property. The first—the Prioritizing Resources and Organization for Intellectual Property Act of 2008[86] (PRO-IP Act)—expands federal jurisdiction over domain names by providing for civil forfeiture proceedings in cases of intellectual property crimes.[87] Interestingly, these crimes need not have any connection with the domain name itself; rather, the statutes are directed toward

---

82 See *Image Online Design, Inc v Internet Corp for Assigned Names and Numbers*, 2013 WL 489899, *2–5 (CD Cal).

83 Id at *8.

84 For example, in March 2015, ".Nissan," ".Datsun," ".Oracle," ".Infiniti," and ".Epson" were added as sponsored gTLDs. See *Delegated Strings* (cited in note 58).

85 See United States Patent and Trademark Office, *Share Comments/Suggestions on Draft of Examination Guide: Applications for Marks Comprised of gTLDs for Domain Name Registration or Registry Services* (Sept 10, 2013), archived at http://perma.cc/3JZW-RY79.

86 Pub L No 110-403, 122 Stat 4256.

87 15 USC § 2323(a)(2).

practices like media piracy, regardless of whether the domain name itself implicates a protected trademark. The second statutory scheme—the Anticybersquatting Consumer Protection Act[88] (ACPA)—largely codifies the trademark protections for subdomains outlined above, but with one important addition: domain names are subject to in rem jurisdiction wherever the domain name registrar or registry is located. These two statutory models provide additional support for a property rights–oriented view of domain names, over and above the support recognized by trademark law.

In 2010, the US government initiated Operation in Our Sites, an enforcement program targeted at websites that illegally host and distribute counterfeit and pirated content.[89] The creation of Operation in Our Sites is authorized by the PRO-IP Act, which provides for the civil forfeiture or destruction of any property used to commit or facilitate certain enumerated intellectual property crimes.[90] To initiate seizure of a domain name, Immigrations and Customs Enforcement (ICE) agents investigate the website in question and then present affidavits to a magistrate. If the magistrate finds probable cause, she can grant a seizure order.[91] This order is presented to the domain name registry located in the United States, and a banner stating that ICE has seized the domain is inserted to replace all content previously on the website.[92] ICE seizures have been heavily criticized in the Internet community, with allegations of due process violations (since seizures proceed ex parte), First Amendment violations, and improper lobbying of ICE by the Recording Industry Association of America, an interest group for music copyright holders.[93]

Importantly, the PRO-IP Act does not explicitly provide that domain names are property subject to seizure. The relevant text of the civil forfeiture statute states that "[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of" certain specified offenses is subject to

---

88 Pub L No 106-113, 113 Stat 1501A-545 (1999).

89 See United States Immigration and Customs Enforcement, *Operation in Our Sites* (May 22, 2014), archived at http://perma.cc/U2FU-YRQM. See also Karen Kopel, *Operation Seizing Our Sites: How the Federal Government Is Taking Domain Names without Prior Notice*, 28 Berkeley Tech L J 859, 860–61 (2013).

90 18 USC § 2323.

91 See Kopel, 28 Berkeley Tech L J at 865 (cited in note 89).

92 For further explanation of the seizure process, see id at 874–77.

93 See, for example, id at 885–93.

seizure.[94] The DOJ and ICE have interpreted § 2323 to include domain names as property,[95] and given the continued practice of domain name seizure under Operation in Our Sites, it appears that a number of federal magistrate judges have agreed with this interpretation.[96]

One other statutory scheme authorizes the seizure and transfer of domain names. In 1999, Congress passed the ACPA to target cybersquatters who opportunistically register infringing domain names. The ACPA is more explicit than the PRO-IP Act regarding domain names' property status, referring directly to "domain names" rather than merely to "property."[97] Further, the ACPA defines domain names as property for the purpose of in rem jurisdiction: if the plaintiff is unable to obtain in personam jurisdiction over the owner of the domain name, he may sue the owner of the domain name in whichever district the domain name registry or registrar is located.[98] The ACPA sends a clear message that if domain names infringe on registered trademarks, the domain name can be seized in a manner that is consistent with traditional notions of property law.[99]

---

94 18 USC § 2323(a)(1)(B).

95 See Brian T. Yeh, *Online Copyright Infringement and Counterfeiting: Legislation in the 112th Congress* *4 (Congressional Research Service, Dec 5, 2011), archived at http://perma.cc/7LKJ-W2SM.

96 These court orders are sealed. However, as noted above, when either the DOJ or ICE wishes to seize a domain name, the agency is statutorily required to seek the authorization of a magistrate. Thus, the continued existence of Operation in Our Sites demonstrates near-universal compliance with these requests on the part of federal magistrates. See, for example, US Department of Justice, *Department of Justice Seizes More than $1.5 Million in Proceeds from the Online Sale of Counterfeit Sports Apparel Manufactured in China* (May 11, 2012), archived at http://perma.cc/77T8-GVWV. Since the inception of Operation in Our Sites in 2010, the DOJ and ICE have seized at least 2,713 domain names. See United States Immigration and Customs Enforcement, *Federal Agencies Seize More than $21.6 Million in Fake NFL Merchandise during 'Operation Team Player'* (Jan 30, 2014), archived at http://perma.cc/5RAC-L5G8. Only a handful of websites have successfully opposed seizure. See *In the Matter of the Seizure of the Internet Domain Name "DAJAZ1.COM"* (Electronic Frontier Foundation), archived at http://perma.cc/EFM2-WD84; Mike Masnick, *Oops: After Seizing & Censoring Rojadirecta for 18 Months, Feds Give Up & Drop Case* (Techdirt, Aug 29, 2012), archived at http://perma.cc/EZ5W-D786.

97 Compare 15 USC § 1125(d)(1)(B)(ii)(C) ("[A] court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark."), with 18 USC § 2323(a)(1) ("The following property is subject to forfeiture to the United States Government: . . . (B) [a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense.").

98 15 USC § 1125(d)(2)(A)(ii)(I).

99 Courts have also authorized seizure of domain names under state statutes. See, for example, *Kentucky v 141 Internet Domain Names*, 2008 WL 5261775, *39–40 (Ky Cir).

For example, in *Office Depot, Inc v Zuccarini*,[100] the Ninth Circuit viewed the ACPA as persuasive authority for the proposition that domain names are seizable property.[101] Office Depot obtained a judgment against the defendant for cybersquatting under the ACPA but was unable to collect and instead assigned the judgment to DS Holdings.[102] DS Holdings then attempted to collect other, noninfringing domain names from Zuccarini. Even though these domain names were unrelated to any action under the ACPA, the court nevertheless held that "the statute is authority for the proposition that domain names are personal property" subject to in rem jurisdiction wherever the registry or registrar is located.[103] Viewed this way, the ACPA supports a concept of in rem jurisdiction based on domain names even when those domain names are not used for cybersquatting or otherwise subject to the provisions of the ACPA.

3. *Kremen v Cohen*:[104] the "intangible property" theory.

Perhaps the strongest theory of domain names as property is articulated in *Kremen*. Gary Kremen registered the subdomain "sex.com," but Stephen Cohen impersonated him in order to convince the domain name registrar to release Kremen's registration; Cohen then registered the subdomain himself and turned "sex.com" into a "lucrative online porn empire."[105] Kremen ultimately prevailed on a conversion claim: Cohen had deprived him of a property interest that he held in the domain name.[106]

The Ninth Circuit reasoned that domain names are intangible property on two grounds. First, "[o]wnership [of a domain name] is exclusive in that the registrant alone" decides where users who type in the domain name are sent.[107] This characteristic is similar to the rights of use and exclusion in the traditional bundle of property rights:[108] a registrant exercises the right to use by deciding what visitors to a web address see and in turn

---

100 596 F3d 696 (9th Cir 2010).

101 Id at 702.

102 Id at 698.

103 Id at 702.

104 337 F3d 1024 (9th Cir 2003).

105 Id at 1027.

106 Id at 1036.

107 Id at 1030.

108 See J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L Rev 711, 756 (1996).

excluding others from making this decision. Second, "like other forms of property, domain names are valued, bought and sold, often for millions of dollars."[109] In other words, domain names are alienable. The right to alienate has long been viewed as one of the fundamental rights associated with property.[110] To the extent that the law recognizes intangible property rights,[111] a "domain name falls easily within this class of property."[112]

The Ninth Circuit's reasoning in *Kremen* is especially important to the question of property rights in TLDs because its identification of a domain name as property did not rest on trademark grounds or on a view that a webpage itself is a property object. Instead, the court viewed a domain name as a "document" or collection of documents in the DNS:

> The DNS also bears some relation to Kremen's domain name. We need not delve too far into the mechanics of the Internet to resolve this case. It is sufficient to observe that information correlating Kremen's domain name with a particular computer on the Internet must exist somewhere in some form in the DNS; if it did not, the database would not serve its intended purpose. Change the information in the DNS, and you change the website people see when they type "www.sex.com."[113]

Recognizing a property interest in what essentially amounts to a line of text in a name server is fundamentally different from recognizing a property interest in a trademark. Unlike a trademark, the protected item need not be "unique" or more than "merely descriptive,"[114] but rather it must simply be something that provides one party exclusivity and control over what is shown to a web address's visitors. *Kremen* should be properly

---

109 *Kremen*, 337 F3d at 1030.

110 See A.M. Honoré, *Ownership*, in A.G. Guest, ed, *Oxford Essays in Jurisprudence* 107, 118 (Oxford 1961).

111 As distinct from tangible property—such as cars, houses, and other objects falling into the categories of real or personal property—intangible property is generally something over which one can have or transfer control but that does not have a physical presence. Some examples include intellectual property rights (such as patents), stock certificates, and bonds. See Restatement (Second) of Torts § 242; Juliet M. Moringiello, *Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future*, 72 U Cin L Rev 95, 124–26 (2003); Courtney W. Franks, Comment, *Analyzing the Urge to Merge: Conversion of Intangible Property and the Merger Doctrine in the Wake of* Kremen v. Cohen, 42 Houston L Rev 489, 502–07 (2005).

112 *Kremen*, 337 F3d at 1033.

113 Id at 1034.

114 See text accompanying note 82.

considered as setting forth a distinct theory of property interests in domain names, and it may be the strongest case yet for recognition of property interests in TLDs.

* * *

Ultimately, then, two broad doctrines support the idea that TLDs could be property. The first, a trademark theory, is relatively straightforward: if TLDs can be source identifying rather than merely descriptive, they can receive certain protections under that doctrine. The second view, that TLDs could be abstract property, is more complex but also more robust. Under this approach, the line of text on a server that either a subdomain or a TLD represents—a line of text in the TLD zone file in the case of a subdomain, or a line of text in the root zone file in the case of a TLD—constitutes intangible property similar to a stock certificate. In other words, the rights conveyed are the *res*, the thing itself, and because these rights potentially include the rights to exclude and alienate, they can be construed as property rights. Nevertheless, the view that treats TLDs as property is not the only view out there. As the next Section demonstrates, an approach treating domain names as services rather than property has emerged to counter the property-oriented approaches described above.

B. TLDs Recognized as Services

The second major line of cases views domain names as services that, by definition, cannot be seized to satisfy tort or contract judgments. It is useful at this point to reiterate the distinction between subdomains and TLDs: while a subdomain points to a unique IP address, a TLD does not. A TLD may contain IP addresses from many different blocks and cannot be separated from the subdomains under it. The service theory of domain names does not always reflect this distinction. But the strongest version of the service theory would rely on the difference between a domain name pointing to a specific webpage and a TLD aggregating a collection of subdomains. The service theory would use this distinction to support the argument that, even if domain names resemble abstract property—as *Kremen* and the other doctrines above would hold—TLDs are more accurately viewed as interconnected service agreements rather than discrete property objects.

1. *Lockheed Martin Corp v Network Solutions, Inc*[115] and *Network Solutions, Inc v Umbro International, Inc*:[116] the service theory.

In *Lockheed*, Lockheed brought an action against NSI for contributory infringement due to NSI's role in providing domain names to various parties who had registered domain names similar to Lockheed's "Skunk Works" trademark.[117] The registrants of the various infringing domain names were numerous and difficult to locate.[118] Lockheed's strategy of seeking injunctive relief against NSI, the relevant DNS-registry operator, raised interesting questions of third-party liability for cybersquatting and Internet trademark violations.[119] Ultimately, the court determined that NSI provided a service—rather than a product—to the registrants of infringing trademarks and therefore could not be liable for contributory infringement.[120] The court analogized domain names to street addresses, explaining:

> NSI's role *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* by performing the routine service of routing mail.[121]

The product/service distinction does not directly map onto the property/nonproperty question.[122] Nevertheless, the two

---

115 194 F3d 980 (9th Cir 1999).

116 529 SE2d 80 (Va 2000).

117 *Lockheed*, 194 F3d at 983.

118 Id.

119 Lockheed also did not have the benefit of the ACPA, which was passed later that year. See note 88 and accompanying text.

120 *Lockheed*, 194 F3d at 984–85.

121 Id (emphasis added).

122 One intuitively appealing approach might be to make a direct comparison between product and property on the one hand, and service and nonproperty on the other. But it is important to keep in mind the context of the *Lockheed* decision. The domain name in *Lockheed* comports with a product/service distinction that constitutes a term of art within the doctrine of contributory infringement. See *Inwood Laboratories, Inc v Ives Laboratories*, 456 US 844, 854 (1982):

> Thus, if a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer

characterizations are conceptually similar, and the metaphor of domain names as street addresses has proven influential and long lasting in the broader debates over domain name law.[123] Of course, street addresses correspond to real property far more concretely. Despite such points of discord, however, the conceptual similarity feels intuitive, and it might appeal to courts given the scarcity of domain name cases.

A similar service theory of domain names was articulated in *Umbro*, in which the plaintiff, Umbro, had obtained a default judgment against a Canadian corporation in a previous action.[124] Umbro sought to enforce the judgment in Virginia state court by garnishing the Canadian corporation's portfolio of valuable domain names and naming NSI as the garnishee.[125] NSI argued that it held no property of the judgment debtor, and it characterized domain names as "standardized, executory service contracts."[126]

The Virginia Supreme Court agreed with NSI, holding that the domain names were not garnishable property.[127] In doing so, the court analyzed the DNS in detail. The court considered the ACPA's recent classification of domain names as property, and it acknowledged the possibility that domain names may be a form of intangible personal property.[128] But what proved most persuasive to the court was the analogy employed in *Lockheed*: the court "[was] cognizant of the similarities between a telephone number and an Internet domain name and consider[ed] both to be products of contracts for services. . . . [N]either one exists separate from its respective service that created it."[129]

The *Umbro* decision should not be read broadly. The holding rests on a narrow issue of Virginia law: the contract for services between NSI and the Canadian corporation was determined not to be a "liability" under one particular statutory provision.[130]

---

or distributor is contributorially responsible for any harm done as a result of the deceit.

Whether the product/service distinction in this area of law is completely coextensive with other conceptions of property/nonproperty is a larger question.

123 See, for example, text accompanying note 149.

124 *Umbro*, 529 SE2d at 81.

125 One of these domain names was "umbro.com"; it appears that the Canadian corporation in question was engaged in cybersquatting. Id.

126 Id.

127 Id.

128 *Umbro*, 529 SE2d at 86.

129 Id at 87.

130 Id at 86.

Additionally, the court explicitly declined to decide whether domain names are a form of intellectual or intangible property, despite NSI's concession that "the right to use a domain name is a form of intangible personal property."[131] The *Umbro* holding, inasmuch as it seems to reject the abstract-property view of domain names advanced by *Kremen*, does so within the bounds of a specific state statutory scheme.

Nevertheless, the conceptualization of domain names as services rather than property objects stands as a powerful counterexample to the trademark protections implied by *In re theDot*,[132] the civil forfeiture implications of the ACPA and the PRO-IP Act,[133] and the abstract-property theory developed in *Kremen*.[134] Although the service theory has limitations in the context of subdomains—for example, Lockheed likely would have won under the ACPA, and *Umbro* relies on a specific set of statutes underlying Virginia creditor-debtor law—those limitations seem less salient in the context of TLDs. Even if subdomains contain property rights (a stance powerfully expressed in *Kremen*), some of those rights are much less apparent for TLDs, which do not point to a particular, unique website. In other words, if subdomains are appropriately treated as abstract property at least in part because of the right to use, then the argument for treating TLDs under the same framework is murky: the "use" of a TLD is primarily the registration of subdomains happening under it. This is much less exclusionary than the concept of using a subdomain, which by its nature within the DNS can belong only to one party.

2. *Stern v Islamic Republic of Iran*:[135] a challenge.

The case posing the greatest challenge to the property status of TLDs is *Stern*. In 2003, Shaul Stern and his coplaintiffs obtained a $109 million default judgment against Iran, Syria, and North Korea stemming from the three countries' alleged

---

131 Id. The *Umbro* court "[did] not believe that it is essential to the outcome of [the] case to decide whether the circuit court correctly characterized a domain name as a 'form of intellectual property.'" Id.

132 See *In re theDot*, 101 USPQ2d at 1068–69.

133 See Part II.A.2.

134 See *Kremen*, 337 F3d at 1030.

135 2014 WL 5858095 (DDC 2014). The plaintiffs have appealed the decision, but as of August 28, 2015, no decision has been rendered. *Stern v Islamic Republic of Iran*, No 14-7203 (DC Cir filed Dec 22, 2014).

involvement in a 1997 Hamas terror attack.[136] The plaintiffs have been attempting to collect from the three countries' assets over the past two decades[137] with little success.[138] Their latest effort involved asking the United States District Court for the District of Columbia to attach property of the three countries allegedly in ICANN's possession; this property consisted of the ccTLDs owned by the respective countries, including corresponding non-Latin ccTLDs.[139]

Stern raises a series of nested questions: Are ccTLDs property subject to attachment? If so, who owns them? If the countries associated with given ccTLDs own some property interest in the ccTLDs, where are the ccTLDs located? What weight should be given to the contractual relations surrounding the ccTLDs, such as the services provided by the individual ccTLD registrars and the subdomain owners who have purchased domain names under the ccTLDs?[140] Regardless of how these legal questions should be answered, many early commentators agreed that the plaintiffs in *Stern* should not prevail: the forced judicial transfer of ccTLDs could potentially wipe out thousands of subdomains registered under the ccTLDs and would run the grave risk of "splitting the root" if name-server operators, regional Internet registries (RIRs), and network providers outside the United States refused to comply with the court's judgment.[141] In other words, the conversation around the case immediately shifted from whether the *Stern* plaintiffs should lose to how and

---

136 See *Campuzano v Islamic Republic of Iran*, 281 F Supp 2d 258, 274–79 (DDC 2003).

137 See, for example, *Rubin v The Islamic Republic of Iran*, 637 F3d 783, 784 (7th Cir 2011).

138 But see Farivar, *ICANN to Plaintiffs* (cited in note 54) (suggesting that the plaintiffs succeeded in collecting against a home in Lubbock, Texas, owned by the former Shah of Iran).

139 See *Stern*, 2014 WL 5858095 at *1. It is not clear what the *Stern* plaintiffs would have done with the ccTLDs if the court had ruled in their favor. It is plausible that the *Stern* plaintiffs simply hoped for leverage to bring Iran, Syria, and North Korea to the bargaining table, but the countries may also have opted to privatize their name servers such that individual ".ir," ".sy," and ".kp" subdomains each pointed to one IP address within the respective countries and another in the outside world—in other words, they could have decided to split the root. See notes 17–18 and accompanying text.

140 While many of these questions are specifically directed to ccTLDs given the context of *Stern*, the same general uncertainty would apply to gTLDs as well.

141 See, for example, Farivar, *ICANN to Plaintiffs* (cited in note 54); David Post, *Are Internet Domain Names "Property"?* (Wash Post, Aug 1, 2014), archived at http://perma.cc/66BH-B3PB.

under what theory ICANN should be able to defeat the attachment attempts.[142]

Ultimately, the district court ruled in favor of ICANN's motion on a narrow version of the service theory.[143] It is worth being precise about what the court decided: under District of Columbia attachment law, ccTLDs "cannot be conceptualized apart from the services provided" by the ccTLD managers and name-server operators around the world, and as a result, ccTLDs are not attachable.[144] But as the *Stern* court noted, "the conclusion that ccTLDs may not be attached in satisfaction of a judgment under District of Columbia law does not mean that they cannot be property. It simply means that they are not attachable property within this statutory scheme."[145] Commentators in the Internet technical community hoping for a broad resolution to the question whether TLDs are property did not find their answer in *Stern*.[146]

Given the importance of the underlying policy considerations, it is worth examining in greater depth the questions unaddressed by *Stern*. ICANN made a number of arguments in response to Stern's motion to attach that directly attacked a conception of TLDs as property, but the court did not reach these arguments in rendering its decision.[147] Ultimately, the relevant arguments can be classified into two categories, neither of which is fully satisfactory.

First, ICANN argued that domain names are categorically not property. To support this point, ICANN relied primarily on the service theory of domains as exemplified by *Lockheed* and *Umbro*: in ICANN's view, domain names are precluded from being categorized as property primarily because "a domain name

---

142 See, for example, Farivar, *ICANN to Plaintiffs* (cited in note 54). It is worth noting that, despite the overall tenor of the commentary, ICANN was not a party to this case. The plaintiffs attached ICANN in an attempt to get at the TLDs; ICANN responded with a motion to quash, the resolution of which is *Stern*. See *Stern*, 2014 WL 5858095 at *2.

143 *Stern*, 2014 WL 5858095 at *3–4.

144 Id at *3.

145 Id at *3 n 2.

146 Nevertheless, some commentators consider this a victory for Internet stability and common sense. See, for example, David Post, *DC Court Rules That Top-Level Domain Not Subject to Seizure* (Wash Post, Nov 13, 2014), archived at http://perma.cc/R3D8-6HL8.

147 See generally Memorandum in Support of Non-party Internet Corporation for Assigned Names and Numbers' Motion to Quash Writs of Attachment, *Rubin v The Islamic Republic of Iran*, Civil Action No 01-1655 (DDC filed July 29, 2014) ("*Stern* Brief").

registration is the product of a contract for services between the registrar and registrant."[148] ICANN then drew on the familiar comparison between domain names and telephone numbers or street addresses from *Lockheed*.[149] As ICANN somewhat correctly and somewhat misleadingly concluded, "[I]n assessing whether domain names . . . can be considered 'property,' numerous courts from various jurisdictions have found that they cannot."[150]

But as noted in Part II.A, a litany of case law and statutory law also points in the opposite direction. "Numerous courts from various jurisdictions" have recognized property interests in domain names, under theories ranging from trademark and civil forfeiture to intangible property. The service theory has its own foothold and, given its origins in the case law, it seems particularly strong in areas such as garnishment and judgment collection.[151] But ICANN's assertion is strikingly inaccurate as an account of the entirety of domain name doctrine, which includes the PTO's recognition of intellectual property interests in TLDs,[152] a statutory scheme under the ACPA and PRO-IP Act that explicitly considers domain names to be seizable property,[153] and *Kremen*'s recognition of a tangible property interest that can be converted and subsequently transferred.[154]

ICANN's related assertions similarly fall flat, including its claims that a ccTLD is "not capable of a precise definition," because it is constantly changing as new subdomains are added and deleted; that a ccTLD has no established market for sale or purchase; and that a ccTLD has no value apart from the routing and administrative services provided by the ccTLD manager.[155] *Kremen* addressed the first point convincingly.[156] Regarding the

---

[148] Id at *11 (quotation marks omitted).

[149] Id at *10–12.

[150] Id at *11.

[151] See Part II.B.1. But see also notes 86–95 and accompanying text.

[152] See Part II.A.1.

[153] See Part II.A.2. To be fair to ICANN, it is not obvious that decisions such as *Kremen* and statutory schemes such as the ACPA and PRO-IP Act, which directly address subdomains, should also apply to TLDs. But the same argument would also apply to *Lockheed* and *Umbro*, two cases that ICANN cites for support. Ultimately, arguments drawing parallels between subdomains and TLDs must account for the breadth of doctrine on the subdomain side—breadth that includes abstract-property theories as well as service theories.

[154] See Part II.A.3.

[155] *Stern* Brief at *10 (cited in note 147).

[156] *Kremen*, 337 F3d at 1035 ("Network Solutions also argues that the DNS is not a document because it is refreshed every twelve hours when updated domain name

second point, TLDs have been bought, sold, and transferred, as the case of Tuvalu and ".tv" (discussed below) makes clear.[157] The last point, that a TLD has no value apart from the services provided by the TLD administrator to the Internet community, seems especially odd given that ICANN recognizes a country's right to designate its own ccTLD manager. Indeed, a sovereign's interest in administering its TLD to certain specifications—for example, excluding noncitizens from registering subdomains—may be at odds with a broader conception of the public interest, which, as expressed by ICANN, is explicitly global.[158]

ICANN's second argument fares no better. Even if ccTLDs are property, ICANN argued, they are not owned by their respective countries.[159] Two principles support this argument. First, ICANN cites internal policy documents, which state that "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 [r]egistry."[160] As ICANN interprets these documents, countries "do not possess the sole power to determine or control what entities will operate the ccTLDs assigned to their countries."[161]

ICANN's citation of this document is misleading. First, it is not at all clear why ICANN's internal policies should have authority, either binding or persuasive, in a US legal proceeding—ICANN is a nongovernmental entity with no delegated legislative powers of its own.[162] Second, the document itself notes that it is "not intended to be binding" on the countries or on ccTLD

information is broadcast across the Internet. . . . [But a] document doesn't cease being a document merely because it is often updated.").

157 See Part II.C.

158 See Part II.C.

159 See *Stern* Brief at *13–16 (cited in note 147).

160 Id at *14 (quotation marks and emphasis omitted), citing Governmental Advisory Committee, *Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains* ¶ 9.1.3 (ICANN, Apr 5, 2005), archived at http://perma.cc/WF8N-DF6U.

161 *Stern* Brief at *14 (cited in note 147).

162 See Froomkin, 50 Duke L J at 71 (cited in note 13). One argument might be that if legal doctrine should generally defer to community norms in the absence of externalities, then ICANN's policies should be persuasive authority given that they ostensibly represent the Internet community's viewpoint. But ICANN has been often criticized as poorly representing community interests in DNS governance. See, for example, John Palfrey, *The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed*, 17 Harv J L & Tech 409, 446 (2004); Feld, *Structured to Fail* at 350, 357–58 (cited in note 22).

registrars.[163] For this guidance to be operative, ICANN would "need both Governments and Registries *voluntarily* to agree to apply them within their legal framework. If either the Government or the registry decide not to adopt the principles, this cannot be held against the registry, and the registry still has a valid existence."[164] ICANN thus explicitly acknowledges that it lacks the inherent authority to impose conditions on a government's administration of its delegated ccTLD. Governments can indeed effectuate transfers of their ccTLDs, either from a trusted nonaffiliated registrar or to a designated private party.[165] ICANN's marshaling of conditions for transfer is applicable only if countries have voluntarily consented to ICANN guidelines; if a country can *voluntarily* enter into an agreement with ICANN, it can also refuse to enter such an agreement and choose to administer its ccTLD as it wishes.[166] The idea that countries refusing ICANN's policies cannot unilaterally control their own ccTLDs is flatly contradicted by both extralegal events sanctioned by ICANN and ICANN's own internal policies.

The second aspect of ICANN's argument is that countries do not have the right to exclude registrants from the ccTLDs, because "the entire premise of a ccTLD is that it *will be used and enjoyed by many* who choose to register, operate and visit domain names within that ccTLD."[167] This argument is flatly contradicted by the practices of major ccTLD registry operators operating with ICANN's support. Canada, for example, disallows registration of domain names for noncitizens, nonresidents, and institutions without a territorial presence in Canada.[168] The United States imposes similar conditions,[169] and the United Kingdom requires that prospective registrants list a UK postal address.[170] On a more basic level, ccTLD domain registrars uniformly impose fees that a registrant must pay either yearly or upon application—or both—to register and operate a particular

---

163 GAC, *Principles and Guidelines* at ¶ 1.3 (cited in note 160).

164 Id (emphasis added).

165 See Part II.C.

166 See Sonbuchner, Note, 17 Minn J Intl L at 196 (cited in note 55).

167 *Stern* Brief at *14 (cited in note 147).

168 See Sarah Georges, *ccTLD Registration Guidelines* (Hover, Jan 8, 2013), archived at http://perma.cc/KLE7-H53N.

169 See *The usTLD Nexus Requirements Policy* (Neustar, 2015), archived at http://perma.cc/7MEG-HJZ3.

170 See *Rules* (Nominet, 2015), archived at http://perma.cc/JFR3-HYZW. Nominet is the ".uk" registry operator.

subdomain.[171] These are all obvious exercises of exclusion, no matter how they are justified.

However, there is a stronger version of ICANN's second argument that, perhaps for policy reasons, ICANN did not make. As noted in ICANN's brief, the United States Department of Commerce retains ultimate control over the root zone file.[172] As a result, ICANN would not be able to transfer the Iranian, Syrian, or North Korean ccTLDs to the plaintiffs without Department of Commerce consent (or a similarly binding court order).[173] The implications of this state of affairs are troubling to the Internet technical community because there is a plausible case to be made that, either de jure or de facto, the US government owns all ccTLDs and gTLDs.[174] This control over the root zone file may have certain advantages—stability, in particular—but Internet advocates bristle at a single government potentially exercising control to the detriment of the global public interest.[175]

Any unilateral action by the US government would run the risk of fracturing the web if the other name-server operators decided to split the root zone file, as Postel briefly attempted to do in the 1990s.[176] While the US government operates the A name server via Verisign, the B through M servers voluntarily synchronize with the A server.[177] Every stakeholder involved wants to avoid the DNS "nuclear option," but nevertheless the name-server operators retain the technical capability to split the root. With this in mind, the legal and normative cases for US-government ownership of ccTLDs are murky.

---

171 See, for example, *Pricing Schedule* (Nominet, 2015), archived at http://perma.cc/6E5Y-RXVV.

172 See *Stern* Brief at *7 ("[T]he U.S. Department of Commerce . . . is responsible for verifying that processing procedures have been followed, and authorising any related changes to the DNS root zone and root zone database.") (quotation marks omitted).

173 See id at *18–19.

174 See Markus Müller, 15 Fordham Intel Prop, Media & Enter L J at 712–13 (cited in note 18).

175 See Sonbuchner, Note, 17 Minn J Intl L at 205–06 (cited in note 55).

176 See Müller, 15 Fordham Intel Prop, Media & Enter L J at 725 (cited in note 18) ("[T]he country-code TLDs are dependent on the root file that is only under U.S. control. . . . [T]he United States, by virtue of its control of the root file, can cause great difficulties for a country by transferring the authority for the country-code TLD to an entity outside that country.").

177 Verisign also operates the J name server. See *J.root-servers.net* (Verisign), archived at http://perma.cc/L4Z4-VA83.

* * *

The precedential development around TLDs has been slow and narrow. Courts addressing TLDs have largely chipped away at small problems involving the particular sets of facts in front of them, and the number of data points is limited. Despite this lethargy, two broad theories have emerged: the intangible property theory (as represented by trademark, civil forfeitures, and *Kremen*) on the one hand, and the services theory (employed by *Lockheed*, *Umbro,* and *Stern)* on the other. Another relevant factor, however, is how these theories are reflected in extralegal practice: ICANN and TLD registries make many decisions without consulting the courts and with varying amounts of input from the Internet community.

C. Extralegal Events

If users and administrators of TLDs have reached a consensus on which property rights accrue in TLDs, the legal system might consider these the norms of the industry.[178] Of course, private TLD transactions may impose significant externalities on third parties, and the law should give deference to insider customs only to the extent that they account for this possibility.[179] Two major extralegal events bearing on these norms are relevant to this Comment. Ultimately, each involves reassigning ccTLD administration under the guise of official ICANN procedures. But the differences in these two developments are key, and they suggest a stronger vision of sovereign rights over ccTLD operation than one might glean from reading ICANN's policy statements.

First, in 2001, Australia successfully petitioned ICANN to reassign the ".au" ccTLD from its incumbent registrar to a new organization, auDA, which was chosen by the Australian government.[180] The incumbent registrar was Robert Elz, a personal friend of Jon Postel who had administered ".au" voluntarily

---

[178] For a discussion of the evolution and value of such norms, see generally Benson, 1 J L, Econ & Pol 269 (cited in note 10).

[179] Property rights serve an important role in recognizing which externalities the legal system forces owners to internalize. See Joseph William Singer, *How Property Norms Construct the Externalities of Ownership*, in Gregory S. Alexander and Eduardo M. Peñalver, eds, *Property and Community* 57, 60–66 (Oxford 2010).

[180] See Internet Assigned Numbers Authority, *IANA Report on Request for Redelegation of the .au Top-Level Domain* (Aug 31, 2001), archived at http://perma.cc/8MAB-5X38.

since its inception. The Australian government's view, adopted by ICANN, was that the ".au" ccTLD "should be managed by an organization formally accountable to the Australian Internet community."[181] There were two major issues with this transfer. The first was that ICANN's internal guidelines seem to require a finding of "misconduct, or violation of [ICANN] policies set forth in this document and RFC 1591 . . . or persistent, recurring problems with the proper operation of a domain."[182] But as ICANN noted, "[T]he .au ccTLD [had] developed well to date under the personal stewardship of Mr. Elz."[183] The second issue was that while ICANN stresses the importance of consulting local Internet users and governing ccTLDs by community consensus,[184] it is unclear whether ICANN consulted anyone other than Elz (who opposed the transfer) and the Australian authorities (who were pushing for the transfer). Despite ICANN's assurance that "there is widespread—nearly universal—support for moving the delegation of the .au ccTLD to an organization permitting broad participation of the Australian Internet community in the development of policy,"[185] one of the most prominent Australian Internet-infrastructure companies expressed serious concerns about auDA (the proposed delegee).[186] Regardless, auDA was deemed the appropriate delegee.[187] The lesson of the ".au" redelegation is that if a country wishes to redelegate its ccTLD registrar, it has at least some authority to do so unilaterally.

The second major event relevant to this Comment is Tuvalu's lease of the ".tv" registration to Verisign.[188] Tuvalu delegated the registry operations of ".tv" to the DotTV Corporation in 1998; Verisign purchased the DotTV Corporation in 2001 for

---

181 Id.

182 Internet Corporation for Assigned Names and Numbers, *ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)* (May 1999), archived at http://perma.cc/7JSW-MKYQ, citing Postel, RFC 1591 (cited in note 1). RFC 1591 lays out the basic design and principles for the DNS. See J. Klensin, *Reflections on the DNS, RFC 1591, and Categories of Domains* (Internet Engineering Task Force Network Working Group, Feb 2001), archived at http://perma.cc/4FT2-PV6B.

183 IANA, *IANA Report on Request for Redelegation* (cited in note 180).

184 See id (discussing the importance of local interests and ICANN participation in cooperative arrangements).

185 Id.

186 See A. Michael Froomkin, *How ICANN Policy Is Made (II)* (ICANN Watch, Sept 5, 2001), archived at http://perma.cc/W3RY-F4HV.

187 See IANA, *IANA Report on Request for Redelegation* (cited in note 180).

188 Verisign operates the ".com" and ".net" gTLDs as well as the A and J name servers. See *Company Information – about Verisign* (Verisign), archived at http://perma.cc/L7EB-GTVS.

$45 million.[189] Although ICANN at one point resisted officializing the transfer to Verisign,[190] Verisign ultimately succeeded in what strongly resembles a purchase of a ccTLD—with the country's consent, of course—despite ICANN's insistence that TLDs cannot be bought or sold. Verisign is now listed as the "technical contact" for the ".tv" ccTLD according to IANA,[191] but it offers registration services and is generally considered the registry operator.[192] Ultimately, it appears that Tuvalu avoided the need for ICANN's approval of the transfer.[193]

The Verisign deal now accounts for a significant portion of Tuvalu's GDP. Estimates range from $2.2 million per year (approximately 6 percent of Tuvalu's annual GDP[194]) to at least $4 million per year (approximately 10 percent of Tuvalu's annual GDP).[195] The ".tv" ccTLD is home to a number of valuable subdomains, chief among them "Twitch.tv" (recently acquired by Amazon for $1.1 billion).[196] Tuvalu and Verisign have built a veritable empire on the back of the ".tv" ccTLD.

The ".au" and ".tv" examples show that certain countries have successfully asserted some forms of property rights in their ccTLDs. It is difficult to read the ".au" redelegation as based on any principle other than Australia's sovereign ability to decide who can administer its ccTLD,[197] and Tuvalu shows the ability of countries to alienate the right of ccTLD administration if they so

---

189 See Noam Cohen, *As Online Video Surges, the .TV Domain Rides the Wave* (NY Times, Aug 16, 2014), archived at http://perma.cc/J9PM-QS62.

190 See Declaration of Charles A. Gomes in Opposition to Special Motion to Strike of Defendant Internet Corporation for Assigned Names and Numbers, *Verisign Inc v Internet Corporation for Assigned Names and Numbers*, Civil Action No 04-1292, *5–6 (CD Cal filed Apr 28, 2004).

191 Internet Assigned Names Authority, *Delegation Record for .TV* (June 19, 2013), archived at http://perma.cc/L9RA-U8F4.

192 See *.TV and .CC Registry Policies* (Verisign, July 29, 2014), archived at http://perma.cc/4VCG-SF4K ("Verisign manages the authoritative registry . . . for all domain name registrations that end in '.TV.'").

193 However, it is not clear whether ICANN has the authority to oppose a ccTLD transfer. See Part II.B.2.

194 See Central Intelligence Agency, *The World Factbook: Tuvalu*, archived at http://perma.cc/N8DM-B6JR.

195 See Metcalf, *A ccTLD Case Study* (cited in note 29).

196 See Nick Wingfield, *What's Twitch? Gamers Know, and Amazon Is Spending $1 Billion on It* (NY Times, Aug 25, 2014), archived at http://perma.cc/H5XF-QD72.

197 As commentators have noted, the question of ICANN control over ccTLD registrars is still largely in flux. See, for example, Sonbuchner, Note, 17 Minn J Intl L at 196 (cited in note 55).

choose.[198] The ".tv" redelegation indicates a potential narrowing of the difference between gTLDs and ccTLDs: the significance of ".tv" in the market for subdomain registration has less to do with anything specifically Tuvaluan and more to do with the commercial value of ".tv" to the broadcast-video market as a whole. At the same time, the movement within gTLDs has been away from a utopian public-interest model and toward a commercially oriented sponsor model, as evidenced by the expansion of gTLD delegations since 2012.[199]

It is important to also note that the Tuvalu example shows that a marketplace and a mechanism already exist for transfer of ccTLDs: although ICANN asserted in *Stern* that no protocol exists for the transfer of ccTLD administration from a country to a third party, these transfers are possible. If property is seen as a bundle of rights including the rights to use, exclude, and alienate (among others), it would seem as though most of these rights belong to countries, despite ICANN's statements of policy.[200]

The picture is less clear for gTLD registry operators. gTLD administration is granted on a contractual basis between the registry and ICANN.[201] While there is only one "owner" of a gTLD, administration of a gTLD comes with stipulations and conditions. Although industry norms provide some guidance on the proper treatment of ccTLDs—one that employs some sort of property rights recognition—there is no easy takeaway for gTLDs.[202] The most that can be said is that ICANN's actual exercise of control over gTLDs is much more pronounced than it is over ccTLDs.

---

198 A gTLD registry would not be able to do what Tuvalu did without first seeking ICANN approval, because even the ccTLDs that have signed agreements with ICANN can nevertheless choose not to follow their stated obligations. See Part II.B.2. In contrast, agreements between gTLD registry operators and ICANN impose significantly more conditions. See Internet Corporation for Assigned Names and Numbers, *Registry Agreement*, archived at http://perma.cc/AXK5-PP7H.

199 See, for example, note 84 and accompanying text.

200 See ICANN, *ICP-1* (cited in note 182).

201 See ICANN, *Registry Agreement* (cited in note 198).

202 Perhaps one takeaway is that ICANN owns all gTLDs—or simply administers them as part of its IANA function contract with the Department of Commerce. While intuitively appealing, this is a proposal that both ICANN and the United States would vehemently deny. See notes 232–33 and accompanying text.

* * *

Returning to the fundamental questions asked by *Stern*—whether a TLD is property, and if it is, who owns it—the case law, statutory frameworks, and extralegal norms do not conclusively support any particular overarching approach. One approach—the *Kremen* abstract-property theory—seems most accurate in certain realms: trademarks, conversions, and maybe ccTLDs more broadly all seem to indicate that TLDs are abstract or intangible property. Another approach—the service theory as developed by *Lockheed* and *Umbro* and later adopted by *Stern*—stands in contrast to the abstract-property theory: within certain statutory frameworks, and especially creditor-debtor law, the web of agreements and interconnections seems to make a property-centric view of TLDs anachronistic. ICANN itself, however, argues for a third theory in *Stern*, which has intuitive appeal but not much practical support: perhaps TLDs are just held in public trust and should not be thought of as legal objects at all. As the next Part will argue, these competing theories of TLDs' property status operate not only on an interpretive level—that is, a level that seeks to harmonize the existing cases, statutes, and extralegal events—but also on a normative one.

III. INADEQUACIES OF EXISTING THEORIES, AND A NEW CONTENDER

It is tempting to view the cases, statutes, and extralegal events discussed above as reconcilable. Each addresses the property status of domain names and TLDs in a relatively narrow context; in addition, theories of trademarks, attachment, and civil forfeiture each impose different standards on property determination. Indeed, no uniform standard for property exists across the legal field.[203] Rather, TLDs may be a kind of quasi property, embodying some but not all of the traditional rights commonly associated with property.[204]

The problem with a piecemeal approach to legal determinations of TLDs' property status is that, outside of the limited contexts that have been addressed by courts so far, investors,

---

[203] Of course, traditional definitions of property—a bundle of the essential rights to use, exclude, alienate, and sometimes destroy—abound. See generally, for example, Penner, 43 UCLA L Rev 711 (cited in note 108).

[204] For other examples of quasi property, see Shyamkrishna Balganesh, *Quasi-Property: Like, but Not Quite Property*, 160 U Pa L Rev 1889, 1894–1909 (2012).

policymakers, and TLD operators cannot be sure of either what they can do with TLDs or how vulnerable they might be to a suit challenging their perceived property rights. For this reason, clarity about exactly which rights are assigned to TLDs is vital. Private parties frequently engage in transactions around existing property entitlements. Pinning down a legal definition will provide stability by allowing parties to better predict where the legal entitlements will fall in cases of dispute, thus enabling better bargaining.[205]

This Part identifies four normative objectives relating to TLDs in order to show how existing solutions fail to account for the breadth of data points relevant to TLDs. These four normative considerations are all important for resolving which theory should prevail, but they may be viewed hierarchically; in particular, this Comment argues that stability of the DNS should be valued highest in any evaluation. Under this framework, four potential theories compete for viability: the abstract-property and service theories identified above, a public-trust theory advocated by ICANN, and a theory that TLDs are similar to FCC licenses. Ultimately, a solution recognizing TLDs as licenses would be the best compromise among competing normative considerations. In practice, ICANN's current approach to granting administrative control over particular TLDs strongly resembles that of the FCC in allocating license rights. Legal doctrine should recognize this similarity and apply elements of FCC license rights to the law of TLDs.

A. Normative Arguments

What policy arguments should inform the categorization of TLDs as property or nonproperty? Among the field of potential considerations, four in particular are most relevant to TLDs: stability, predictability, community interest, and descriptive accuracy.

The first two considerations, stability and predictability, are interrelated: given the massive investment in domain names by intellectual property holders and the growth of e-commerce generally, any solution that decreased Internet stability would have significant social costs. Similarly, the Internet as a whole

---

[205] For a discussion on entitlements and bargaining, see Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv L Rev 1089, 1093–95 (1972).

creates a social surplus: everyday users of the network gain enormous benefits from the communication and interconnection that an open Internet enables, so some way of ensuring recognition of community interests in the DNS is vital. Finally, the legal regime surrounding TLDs should aim to be descriptively accurate in order to avoid creating counterproductive legal rules or alienating global Internet stakeholders.

The major normative argument against recognition of a property interest in TLDs is that the forced transfer of TLDs could jeopardize both Internet stability and the unity of the web.[206] Name-server operators, ccTLD registrars, and local Internet service providers could refuse to comply with US court orders—in short, they could split the root. If this were to happen, the Internet would devolve into two internets: name servers complying with US court orders, and name servers not complying.[207] The worst-case scenario for the DNS—in which users of different networks can no longer communicate directly—will have come to pass. ICANN's governance of the Internet rests on a fragile consensus, and if US law takes an aggressive stance on the property status of TLDs, the future of the open Internet could be jeopardized.

A second, related normative principle is the need for predictability. Of course, a stable DNS would be predictable. But a DNS that has some unstable characteristics—for example, one in which TLDs occasionally fold or transfer against the wishes of the subdomain owners underneath it—could nevertheless also be predictable. And conversely, because TLDs may not be created equally with respect to their perceived stability, an unpredictable system might lead subdomain owners toward TLDs about which they have the most knowledge—regardless of whether that migration is an overall social good. For example, a ".tv" TLD might give more information to a consumer in the case of a media company, but if the media company cannot predict the future existence of ".tv," this information benefit may not occur. Transfer of a TLD could wipe out subdomains underneath it,[208] which would discourage investment in domain

---

[206] See Feld, *Structured to Fail* at 357 (cited in note 22).

[207] ICANN does have contracts with name-server operators, regional Internet registries, and some ccTLD administrators that bind them to synchronize with the A server. See id at 349–50. Enforcing these contracts, however, runs into the same issues as enforcing a court order.

[208] See Farivar, *ICANN to Plaintiffs* (cited in note 54).

names. Concerns over uncertain potential transfers of ccTLDs might encourage companies to migrate to gTLDs or to whichever TLDs are seen as the most stable, whether generic or country code.[209]

If consumers of domain names view the stability of various TLDs as unpredictable, centralization may occur. For example, if the founders of Twitch.tv had felt concern over the status of the ".tv" domain, they may have opted to launch their site on a TLD whose future existence was more certain. Centralization of domain name registration increases costs to companies and reduces consumers' access to information. If every company were compelled to register a ".com" subdomain, for example, these subdomains would become extremely expensive compared to identical subdomains on different TLDs.[210] New ventures would face increased barriers to entry as prime subdomains all become registered. Because subdomains communicate information about a business or entity to Internet users, too much concentration in, for example, ".com" hurts consumers' ability to gather information about the companies with which they wish to transact.[211] The entire Internet benefits from predictability in the DNS in the form of reduced costs to domain name registrants and increased information gains to Internet consumers.

A third normative consideration asserts that because the smooth operation of the Internet relies on the consent and cooperation of various global stakeholders, decisions about property rights should recognize the interests of the Internet community.[212] The Internet community at large is not necessarily

---

[209] For more on the economic value of legal certainty, see Nestor M. Davidson, *Property's Morale*, 110 Mich L Rev 437, 445–47 (2011).

[210] Verisign's market power over the DNS as registrar of the ".com" gTLD has been criticized as monopolistic. See, for example, Smith, 20 Richmond J L & Tech at 17 (cited in note 62). However, the new gTLD program has aimed to increase competition in the gTLD namespace. See Internet Corporation for Assigned Names and Numbers, *About the Program* (2015), archived at http://perma.cc/3HS8-2ZS5. Early signs indicate success: new gTLDs have accounted for over 6.5 million new domain name registrations since 2014. See *nTLDStats* (greenSec Solutions, 2015), archived at http://perma.cc/DX3B-UHZZ. Additionally, ".com" faces competition from ccTLDs such as ".tv" that aim toward commercial use outside their countries of origin. See, for example, DomainWire, *Domain Name Stat Report* *2 (Council of European Top level Domain Registries, May 2013), archived at http://perma.cc/77FX-X877 (noting that in 2013, ccTLD registration was up 12 percent, as compared to 2 percent across gTLDs).

[211] See Jessica Litman, *The DNS Wars: Trademarks and the Internet Domain Name System*, 4 J Small & Emerging Bus L 149, 157–59 (2000).

[212] See Vint Cerf, Patrick Ryan, and Max Senges, *Internet Governance Is Our Shared Responsibility*, 10 I/S: J L & Pol Information Socy 1, 3–4 (2014).

coextensive with the group of stakeholders who have the de facto power to resist judgments or become parties to litigation involving TLDs: RIRs, name-server operators, TLD registries, and Internet service providers could each undermine Internet stability, but the consent of Internet *citizens* and subdomain owners is not required. This result is at odds not only with utopian conceptions of the Internet—such as those defining TLDs as community property—but also with more conservative stances emphasizing the consequences of poor governance to individual Internet users.[213] Put another way, governance of the TLD namespace involves significant risks of externalities to Internet users, recreational and corporate alike. DNS management should internalize these risks.

However, this view should not be taken too far. A normative theory that TLDs are property only insofar as they are *community* property must wrestle with the fact that some body or process must exist to resolve disputes over DNS control (even if this "control" is not labeled as "ownership").[214] ICANN may or may not be the best problem solver, but the nature of the DNS does not allow for pure decentralization. Someone must administer the root zone file to prevent the constant addition, deletion, and transfer of TLDs.[215]

Finally, legal doctrine involving TLDs and property rights should be descriptively accurate regarding the technical practices of the DNS. Descriptive accuracy aids legitimacy; a court order that does not appear to understand the technology runs an increased risk of enacting counterproductive legal rules and alienating Internet stakeholders.[216] Further, descriptive accuracy helps courts know when to distinguish different aspects of the DNS and when to change the doctrine in cases of technical

---

[213] See, for example, Michael Xun Liu, Note, *Jurisdictional Limits of* In Rem *Proceedings against Domain Names*, 20 Mich Telecomm & Tech L Rev 467, 491 (2014) (noting that "the exercise of *in rem* jurisdiction under the ACPA also harms individual interests by undermining party expectations and creating procedural unfairness for foreign litigants").

[214] See Goldsmith and Wu, *Who Controls the Internet?* at 31 (cited in note 26).

[215] See id at 32.

[216] See, for example, *Kentucky v 141 Internet Domain Names*, 2008 WL 5261775, *15–22 (KY Cir). The court in *141 Internet Domain Names* found that domain names were property located in the Commonwealth of Kentucky because the domain names were listed on interfaces (webpages) shown to web users in Kentucky, describing the domain names as "virtual keys for entering and creating virtual casinos." Id at *23. For a longer discussion of the weaknesses of this opinion, see Mellyn, 42 Georgetown J Intl L at 1251–53 (cited in note 63).

innovation or new business arrangements. Descriptive accuracy may simply be seen as an end in itself—a legal system too formal and too far removed from business practice is a bad result even without consideration of the potential negative consequences.

There may, of course, exist further normative considerations through which to evaluate the potential theories underlying the legal status of the DNS. This Comment does not attempt to develop an exhaustive list. Instead, the four considerations identified above—stability, predictability, community interest, and descriptive accuracy—are included as a reflection of priorities.

B. Evaluation of Competing TLD Theories

With these four considerations in mind, it is now possible to evaluate the various theories of TLD property rights against a normative backdrop. No theory perfectly accounts for all potential considerations. However, any evaluation of which theory is best suited for widespread adoption by US courts should explicitly weigh these normative principles against each other. In particular, this Comment argues that stability—specifically, avoiding splitting the root—should be recognized as the primary consideration for the various theories of TLDs' property status. In part because existing theories do a poor job of accounting for stability, courts should look to FCC licenses as an exemplar. As seen below, ICANN's current policies on TLDs strongly resemble a license model; they strike a balance between public obligation and private rights that deftly solves the problems presented by the four normative considerations identified in this Comment.

1. Shortcomings of the service theory.

The service theory of TLDs fares reasonably well with reference to the normative considerations discussed above. The main advantage of this theory is that it keeps in full view the web of interdependencies on which the Internet rests.[217] This advantage should not be understated: litigation is often an ineffective tool with which to make policy decisions about TLDs and property rights, because people and entities who are not parties to the litigation will tend to be underrepresented. The service theory helps safeguard against a judicial system in

[217] See Cerf, Ryan, and Senges, 10 I/S: J L & Pol Information Socy at 2–4 (cited in note 212).

which courts consider only the present parties rather than making broad, legislative decisions—largely because under the service theory, plaintiffs are unlikely to seek transfer of TLDs given their low chances of victory.

The service theory also aids stability and predictability in a narrow sense: it prevents bad results in some cases, such as the possibility in *Stern* of the Iranian, Syrian, and North Korean ccTLDs transferring to the plaintiffs.[218] But this results-oriented view obscures the possibility that a service theory could prove *less* stable in a number of plausible cases. ICANN could redelegate a ccTLD registrar for political reasons if pressured by its Governmental Advisory Committee (the mouthpiece of different national governments within ICANN, known as "GAC") or by the US government.[219] Indeed, ICANN's actions in the past have been criticized as promoting certain policy goals at the expense of Internet stability.[220] If the legal system were to recognize a property interest in TLDs, a powerful set of entities—countries, designated ccTLD registrars, and the companies that operate gTLD registries—would be given incentives and entitlements to resist any political moves by ICANN that might jeopardize the community-property nature of the DNS and the Internet generally. The question is less whether ICANN is trustworthy and more how to structure Internet governance to prevent one organization from gaining too much control over critical Internet infrastructure. Thus, a major failing of the service theory as compared to regimes that recognize stronger rights for TLD operators is that it fails to provide a check on the power of whatever central authority retains control over the DNS—whether that is ICANN now or another organization in the future.

Similarly, the service theory of TLD ownership fails to account for situations like *Kremen* in which a major injury occurs because of a TLD owner but in which that party's only major asset is the TLD itself.[221] What would happen if Verisign went bankrupt or committed major financial fraud?[222] How would

---

[218] See *Stern*, 2014 WL 5858095 at *3. See also Part II.B.2.

[219] According to some commentators, ICANN has already done so. See, for example, Froomkin, *How ICANN Policy Is Made* (cited in note 186); Feld, *Structured to Fail* at 350 (cited in note 22).

[220] Feld, *Structured to Fail* at 350 (cited in note 22).

[221] See *Kremen*, 337 F3d at 1026–28.

[222] Verisign does receive revenue from services apart from its registry operations, but the right to administer the ".com," ".net," and ".tv" registries, among others, is one of Verisign's most significant assets. See Verisign, Inc, *Form 10-K: Annual Report pursuant*

ownership of the ".com" TLD be resolved under the service theory? The service theory of TLD ownership does not satisfactorily account for this scenario.

A third major failing of the service theory is that it simply is not an accurate description of what a TLD is.[223] To be sure, operation of a TLD registry involves providing services to registrars and subdomain registrants, and a TLD is valid only insofar as the thirteen name servers contain entries recognizing the TLD and its registry; that is, a TLD has content only when it both is recognized under the DNS and itself recognizes subdomains.[224] The fact that services are necessary to establish value in an object is not dispositive of whether the underlying object contains a property interest. The same service/property interactions exist in trademarks and patents, for example.[225] Simply because a good requires certain services to be performed in order to become socially valuable does not preclude it from being considered property.

2. Shortcomings of the abstract-property theory.

The abstract-property theory of TLDs has a conflicting but overlapping set of normative concerns at its core. Accepting *Kremen*'s reasoning as applied to subdomains—in short, that the rights to use and exclude as they relate to a line on a name server are enough to qualify subdomains as abstract property—it is difficult to see why TLDs should not be viewed in the same way. A reserved line on a name server that grants the rights to use, exclude, and alienate constitutes abstract property regardless of whether it is called a subdomain or a TLD. To be sure, subdomains are distinguishable from TLDs in that each subdomain points to a unique IP address; a TLD divorced from the subdomains it contains does not.[226]

---

to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2014 (SEC, Feb 13, 2015), archived at http://perma.cc/3NWD-XACP; *Company Information – about Verisign* (cited in note 188).

[223] By comparison, *Kremen*'s recognition of the value of a subdomain—controlling what an end user sees when visiting a web address—seems to accord better with common understandings of property. See *Kremen*, 337 F3d at 1030.

[224] See Milton L. Mueller, *Internet Governance in Crisis: The Political Economy of Top-Level Domains*, archived at http://perma.cc/6YEB-B786.

[225] See notes 117–21 and accompanying text.

[226] This distinction is not as minor as it might seem. The primary use of a subdomain is to point end users to a viewable webpage; their property relevance largely arises from the subdomain owner's right to direct the end user wherever the owner chooses.

But it is far from self-evident that this distinction is legally relevant. The rights exercised by a subdomain owner and the rights exercised by a TLD administrator are not fundamentally different. The TLD administrator may be bound by a contract with ICANN to charge a fixed price for subdomain registration—though this requirement is crumbling under the latest version of the gTLD registry and registrar contracts.[227] But the fact that ICANN needs to impose these limitations of rights via the contract form implies that a TLD administrator could exercise them in the first place. Some version of the *Kremen* analysis, then, would seem to apply to TLD registrars and registry operators, given their apparent rights. For this reason, abstract property is simply a more accurate definition of what ccTLDs are.

Unfortunately, the abstract-property theory fares poorly on the other normative considerations. The difficult question for proponents of an abstract-property theory is what to do with *Stern*. As shown in Part II.B.2, the consequences of allowing the *Stern* plaintiffs to seize the ".ir," ".sy," and ".kp" ccTLDs would have been severe, potentially crippling Internet stability and the unified web. The abstract-property theory as expressed in *Kremen* struggles to come up with a principle preventing this seizure.[228]

One approach might be to say that even if TLDs are some kind of intangible property, the existing statutory schemes of attachment and garnishment do not allow for seizure of that property form. This approach has the advantage of reconciling *Kremen* with the *Lockheed-Umbro-Stern* line of cases, which explicitly declined to comment on the broader definitional concerns this Comment addresses. In other words, by focusing on the narrow nature of each decision, this approach avoids conflict: TLDs are one thing for the purposes of attachment in the District of Columbia or Virginia, another thing for conversion in California, and another thing in the patent context.

But accepting this argument essentially leads back to square one. If TLDs are some kind of abstract property with some features of nonproperty, courts will have difficulty deciding when and under what contexts TLDs should receive property

---

TLDs have no comparable function. See Mueller, *Internet Governance in Crisis* (cited in note 224).

[227] See ICANN, *2013 Registrar Accreditation Agreement* (June 27, 2013), archived at http://perma.cc/6RK4-JZSR.

[228] See *Kremen*, 337 F3d at 1033–34.

protection. This difficulty may lead to anomalous results that undermine the general stability and predictability of the domain name system. If parties cannot predict what courts will do when questions regarding the property status of TLDs arise in litigation, they will struggle to arrange their affairs and manage the potential risks of investing in subdomains under a particular TLD. In other words, the abstract property theory has trouble drawing lines with regard to what property protections are afforded to TLDs. Of course, a rights regime could be stable despite taking an ad hoc, piecemeal approach, assuming that parties know which contexts are protected and which are not. But this seems unlikely from a practical perspective. The question of property protections for TLDs could come up in numerous legal contexts, each of which would have to be resolved individually by different jurisdictions. And while these cases are pending, industry participants and policymakers will have to make decisions on where to invest and what types of regulatory actions to take—all of which could be undermined.

Another problem with the abstract-property theory is that it fails to account for the Internet community's interest in a particular TLD. By its very nature, the abstract-property theory recognizes a strong version of the right to exclude that is incompatible with a community-interest norm. If the TLD owner's property interest subordinates the rights of the subdomain owners relying on the TLD registry, subdomain owners will be at the whim of the country's or registry operator's business decisions and debts. For example, if Verisign makes a bad investment in a major infrastructure project and declares bankruptcy, secured creditors will have an entitlement over the billions of subdomain owners under ".com" and ".net," as well as the other TLDs operated by Verisign. This is especially problematic for TLDs because the sheer number of subdomain owners affected by a seizure of ".com" presents intractable collective action problems precluding efficient bargains between subdomain owners and creditors. The community interest in TLDs is not an expression without content; rather, it reflects the real issues presented by the open, international nature of the Internet.

3. A third contender: ICANN's public-trust theory.

If neither the abstract-property theory nor the service theory of TLDs is normatively acceptable, are there alternative theories, not yet recognized by courts, that might better protect the

interests of stability, predictability, community interest, and descriptive accuracy recognized above? One potential theory would be ICANN's stance that TLDs are operated "in trust in the public interest."[229] This public-trust theory has not explicitly been advanced as a theory of property by ICANN, but in its strongest form it holds that TLDs are common resources that, by their very nature, should be operated by consensus in the interests of the community, including both current participants and future Internet users.[230] What exactly a "public trust" is in this context is undeveloped but might be analogized to national parks or public waterways: social welfare is maximized by some baseline rules, but no private rights are recognized.[231]

The public-trust theory has a few strengths. First, it gives credence to the community-interest norm. Even more than the service theory, the public-trust theory accounts not only for the web of interdependent name servers and TLD administrators but also for current and future Internet users. Similarly, the public-trust theory recognizes the value of DNS stability, because any disruptions or fractures in the DNS would be welfare decreasing.

However, the public-trust theory is not uniformly superior to the service theory or the abstract-property theory on the normative bases identified. One issue is that if the DNS is operated in the public trust, it is unclear why the DNS should not be in government hands. Notably, ICANN and many stakeholders—including the US government—sharply disagree with this conception.[232] The United States in particular has increasingly denied control over the DNS, perhaps in response to criticism in the international community of its influence on ICANN policy.[233]

---

[229] *Stern* Brief at *14 (cited in note 147) (quotation marks and emphasis omitted).

[230] See id at *13–14; GAC, *Principles and Guidelines* (cited in note 160).

[231] See, for example, Federal Land Policy and Management Act § 102(a)(8), Pub L No 94-579, 90 Stat 2743, 2745 (1976), codified at 43 USC § 1701(a)(8):

> [T]he public lands [shall] be managed in a manner that will protect the quality of scientific, scenic, historical, ecological, environmental, air and atmospheric, water resource, and archeological values; that, where appropriate, will preserve and protect certain public lands in their natural condition; that will provide food and habitat for fish and wildlife and domestic animals; and that will provide for outdoor recreation and human occupancy and use.

[232] See White Paper, 63 Fed Reg at 31742–44 (cited in note 49) (arguing for and explaining the transition to private management of the DNS).

[233] See Geoff Duncan, *Why Is the U.S. Surrendering Control of the Internet? (And Why Should You Care?)* (Digital Trends, Mar 19, 2014), archived at http://perma.cc/6UBL-XACP.

One answer to why the DNS should be kept out of government hands might be that the DNS is a global system. The main functions of the DNS—providing unique domain names for IP addresses and ensuring uniformity across the various name servers—address global issues.[234] But this rejoinder raises questions of ICANN's authority as well as its origin. As a nonprofit incorporated in California, ICANN was founded through US initiative and remains subject to US jurisdiction.[235] If the DNS is truly a global public good, perhaps it should be either operated by an international body such as the United Nations or operated similarly to other international agencies.[236]

The other disadvantage of the public-trust theory is that it adds little predictability to the DNS. ICANN's corporate structure is arcane and provides no easy answers as to who actually makes decisions or what weight should be given to the views of particular stakeholders.[237] Given the complexity of property interests, it is difficult to predict what factors ICANN will consider or what norms ICANN will value in making decisions.[238] Perversely, predictability is improved in the current system only if ICANN operates poorly: if we know that ICANN will always be swayed by whatever countries are able to exert the most political pressure or that the GAC will be deadlocked by a power struggle, commentators could foresee with some accuracy how particular problems will be resolved. But the actual resolutions might continue to be at odds with the interest of the general Internet community.[239]

The service theory, abstract-property theory, and public-trust theory are in some sense philosophically in tension with each other: ultimately, they take fundamentally different

---

[234] See Shackelford and Craig, 50 Stan J Intl L at 129–30 (cited in note 39).

[235] See White Paper, 63 Fed Reg at 31741 (cited in note 49). See also *Stern*, 2014 WL 5858095 at *2.

[236] This is essentially what the Generic Top-Level Domain Memorandum of Understanding proposed. See The Internet Community, *Establishment of a Memorandum of Understanding* (cited in note 38).

[237] See Froomkin, *How ICANN Policy Is Made* (cited in note 186).

[238] Interestingly, ICANN has also identified predictability and certainty as core normative considerations when discussing the gTLD expansion project. But commentators have noted that the gTLD application process has been anything but stable or predictable. See, for example, Michael D. Palage, *ICANN's New gTLD Double Standard?* (CircleID, Mar 1, 2011), archived at http://perma.cc/HFV7-A62X. Michael D. Palage was a member of the ICANN Board of Directors from 2003 to 2006. See Internet Corporation for Assigned Names and Numbers, *Board of Directors*, archived at http://perma.cc/RLW6-9NGV.

[239] See, for example, Froomkin, *How ICANN Policy Is Made* (cited in note 186).

approaches to the treatment of TLDs. For this reason, each theory carries different sets of normative strengths and weaknesses. The service theory excels at providing stability—conditioned, of course, on good stewarding by the organizations in charge of the DNS—but is less descriptively accurate and provides no built-in mechanism for community input. The abstract-property theory, on the other hand, seems to match up well with how courts and private parties have treated TLDs in the past, but it could be disastrous to Internet stability if not tempered. Finally, the public-trust theory is the only one to explicitly recognize the importance of the public's interest in TLDs and the DNS generally, but it fails to account for the other two concerns. As mentioned above, it is possible that no theory will satisfactorily address each concern. This Comment argues that viewing TLDs as similar to FCC licenses does a better job of accounting for stability, predictability, community interest, and descriptive accuracy on the whole than any of the theories listed above.

4. TLDs as licenses.

FCC licenses strike a unique balance between a public-trust theory of property rights and a private ownership model. Originally, wireless-spectrum regulation was explicitly oriented toward public-trust norms: as the Supreme Court interpreted the Communications Act of 1934,[240] "[t]he purpose of the Act was to protect the public interest in communications."[241] Today, however, licenses incorporate aspects of private ownership. The rights to use particular spectrum allocations are auctioned off through competitive bidding,[242] and a "shadow market" has emerged for licensees to transfer the grant of spectrum.[243]

FCC broadcast licenses authorize an entity to use a specific frequency in the communications spectrum for a limited time—seven years for radio, five years for television. The vast majority of broadcast licenses are renewed at the end of their terms.[244]

---

240 Pub L No 73-416, 48 Stat 1064, codified as amended at 47 USC § 151 et seq.

241 *Scripps-Howard Radio, Inc v Federal Communications Commission*, 316 US 4, 14 (1942).

242 See, for example, 47 USC § 337(a) (stating that "the Commission shall allocate [a portion of] the electromagnetic spectrum between 746 megahertz and 806 megahertz . . . by competitive bidding"); 47 USC § 309(j) (protecting the "[u]se of competitive bidding").

243 Krystilyn Corbett, Note, *The Rise of Private Property Rights in the Broadcast Spectrum*, 46 Duke L J 611, 638 (1996).

244 See Bruce E. Rosenblum, *Structuring and Restructuring Secured Loans to Broadcasters*, 1 J Bankr L & Prac 271, 272 (1992).

Licensees may not freely transfer their rights but may apply to the FCC to initiate transfers to third parties.[245] Licenses grant usage rights, of course, but these may be proscribed by the FCC; the FCC can also limit the times of day during which a licensee may broadcast.[246]

In the abstract, the FCC restricts access to a medium of communication to maintain uniformity, prevent market confusion, and solve a collective action problem that engenders high transaction costs. This description applies similarly to ICANN's agreements with TLD registry operators and registrars. Thus, TLD-registry contracts may be viewed as the Internet parallel of broadcast licenses: ICANN and the Department of Commerce grant certain private rights to the TLD registrar, such as the right to exclude and the right to alienate subdomains, while retaining a public right to regulate the TLD namespace more generally.[247]

Put more concretely, the license theory states that ICANN's contracts with TLD administrators are not mere service agreements with no attached private rights passing to the registrars, as spectrum licenses were under the old Communications Act of 1934 model; nor are they grants of property with all traditional rights attached, as some commentators wish to see today with FCC licenses.[248] Rather, ICANN grants licenses that convey certain private rights while withholding or conditioning the use of others.[249] These licenses are not freely transferable—for example, Verisign cannot simply sell off ".com" without ICANN's approval[250]—but licensees may use, exclude, and sell subdomains with relative freedom and exclusivity within their granted

---

245 See 47 USC § 310(d).

246 See 47 USC § 308(b).

247 For a more in-depth discussion of broadcast licenses, see Rosenblum, 1 J Bankr L & Prac at 272–74 (cited in note 244).

248 For example, ccTLDs' registry agreements grant registrars certain private rights, such as the right to exclude. Many countries impose geographic or citizenship requirements on prospective ccTLD subdomain registrants. See Part II.B.2.

249 FCC broadcast licenses operate similarly. Regulations prohibit the assignment of FCC licenses but allow the licensee to initiate a process for transferring control over a broadcast license subject to FCC approval. See 47 USC § 310(d).

250 ICANN conditions the grant of registry status for gTLDs on a lengthy agreement with numerous restrictions placed on the gTLD registry operator. For example, gTLD registry operators must price registrations and renewals in certain ways, and they must seek ICANN approval for policy changes. Importantly, gTLD registry operators are not free to transfer the registry to a third party without ICANN approval. See ICANN, *Registry Agreement* (cited in note 198).

spheres.[251] Licensees are simultaneously both market participants bargaining for rights with ICANN and public trustees subject to price restrictions and nondiscrimination policies.[252]

As a descriptive matter, it is important to separate the posturing of stakeholders from the facts of the situation. Despite protestations to the contrary—both from the Internet community and the relevant parties—the United States holds de facto power over the DNS.[253] This is true regardless of whether the United States' control is normatively desirable. Thus any solution that attempts to circumvent the essential facts of root zone file control—such as ICANN's public-trust theory, which by implication denies the hierarchical nature of the DNS—into something more palatable to government skeptics runs headfirst into reality. Keeping Internet infrastructure outside the territorial jurisdiction of individual governments might be a better system, but it is not the system in place today.[254]

Keeping this in mind, a license system does a better job of describing TLDs' property status as expressed by extralegal transactions than either the pure abstract-property theory, the service theory, or the public-trust theory does. Broadcast licenses are not directly reachable by creditors,[255] and their transfer is conditioned on FCC approval.[256] This arrangement also accurately depicts the property dynamic expressed on the one hand by *Stern* and on the other by the Tuvalu and Australia redelegations. It seems clear that the *Stern* outcome, although perhaps cast in terms that are too narrow, is the best possible normative outcome:[257] ccTLDs should not be reachable by creditors or else the stability of the Internet will be jeopardized.[258] Similarly,

---

[251] See id. ccTLD registrars have much more freedom to manage their registries than gTLD registrars do. See GAC, *Principles and Guidelines* (cited in note 160).

[252] For an argument that FCC broadcast licenses strike a balance between the public rights and private rights models of ownership, see Corbett, Note, 46 Duke L J at 634 (cited in note 243).

[253] See Part I.B.

[254] Note that under both Operation in Our Sites and *Stern*, actions to initiate transfer of a domain name or TLD can be litigated only in US courts because ICANN and the major TLD registries are both located within the United States. See Part II.A.2 and Part II.B.2.

[255] See Rosenblum, 1 J Bankr L & Prac at 274 (cited in note 244).

[256] See J. Armand Musey, *Broadcasting Licenses: Ownership Rights and the Spectrum Rationalization Challenge*, 13 Colum Sci & Tech L Rev 307, 327 & n 74 (2012).

[257] See Post, *DC Court Rules That Top-Level Domain Not Subject to Seizure* (cited in note 146) (claiming that the decision reached by the court was "the right result for many reasons").

[258] See Part II.B.2.

countries like Tuvalu that wish to lease a ccTLD to a third party should have some rights to do so, subject to public-interest restrictions.[259] The license theory of TLDs thus checks many of the important boxes under an outcome-oriented analysis.

One concern with the license theory might be that private licenses—licenses between two private parties, as distinct from public licenses granted by a government—might be subject to certain assignability principles that are too permissive when applied to TLDs. For example, the United States Bankruptcy Code allows a trustee to freely assume executory contracts, subject to few restrictions—none of which seems to apply to TLDs.[260] Executory contracts—those in which both sides have important performance obligations remaining[261]—are an obvious target for TLD policy. If, as presented in the hypothetical above, a TLD registry operator were to go bankrupt, both its contract with ICANN and its numerous contracts with subdomain owners would be considered executory contracts. But ICANN imposes restrictions on TLD registry operators that potentially none of the trustees would be able to satisfy.[262] Both ICANN and most likely all the subdomain owners would prefer that ICANN step in and delegate the registries' obligations to a solvent, already-trusted registry operator.

In contrast, public licenses such as FCC broadcast licenses are not generally assumable in bankruptcy; creditors can take an interest in the economic value generated by public licenses, such as proceeds from sale, but because the FCC must approve any transfer of a broadcast license, courts have wisely avoided intruding on that process.[263] Courts should take a similar stance when it comes to ICANN and TLDs. Although ICANN is

---

259 See Part II.C.

260 There are limitations to this doctrine: 11 USC § 365(c) specifies that executory contracts cannot be assigned when applicable law excuses a party other than the debtor from rendering third-party performance, when the contract is for a loan, or when the contract is for nonresidential real property and has been terminated prior to bankruptcy. 11 USC § 365(c).

261 See Bob Eisenbach, *Executory Contracts – What Are They and Why Do They Matter in Bankruptcy?* (In the (Red), July 18, 2006), archived at http://perma.cc/N5R2-LNGW.

262 See *Registry Agreement* (cited in note 198).

263 See *In re Ridgely Communications, Inc*, 139 Bankr 374, 379 (Bankr D Md 1992) ("The right of the licensee crucial to this decision . . . is the right of the creditor to claim proceeds received by the debtor licensee from a private buyer in exchange for the transfer of the license to that buyer."); *In re TerreStar Networks, Inc*, 457 Bankr 254, 262–65 (Bankr SDNY 2011) (providing an overview of doctrinal issues in bankruptcy-related assignation of FCC licenses).

a private nonprofit, its main function is execution of a government contract,[264] and it imposes transfer requirements on TLDs similar to those that the FCC imposes on broadcast licenses.

A second concern might be economic. Just as Professor Ronald Coase and others have argued for a market-based approach to broadcast licensing,[265] a better way to handle TLD registration might be to let firms bid on, sell, and otherwise freely alienate TLD registration licenses. ICANN's approach has more closely resembled the old FCC methods—something like central planning.[266] A common objection might then be that if ICANN's TLD agreements are similar to broadcast licenses, ICANN should more closely follow the FCC's trajectory over the past half century and move to a more market-based model.

It is true, however, that the FCC, while adopting some aspects of a market approach, has retained other centralized characteristics. As mentioned above, the transfer of a broadcast license is conditioned on FCC approval.[267] Further, ICANN must navigate the international nature of Internet infrastructure in a way not required of the FCC. If, for example, ICANN auctioned off ".sy" and the company that bought it announced that it would not renew subdomain agreements with Syrian clients, a potential response from Syria would be to simply split the root: ".sy" would point to one thing within Syria and another thing everywhere else.[268] This scenario—splitting the root—is essentially the nuclear winter of domain name policy.[269] ICANN and other important stakeholders are wise to choose paths that avoid this outcome.

In this way, the license model shares some of the same potential issues as the service model: it places significant trust and

---

[264] See Internet Corporation for Assigned Names and Numbers, *Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers* (Sept 30, 2009), archived at http://perma.cc/B9XM-9NLY.

[265] See generally, for example, R.H. Coase, *The Federal Communications Commission*, 2 J L & Econ 1 (1959).

[266] For a comparison of ICANN and FCC policies, see Karl M. Manheim and Lawrence B. Solum, *An Economic Analysis of Domain Name Policy*, 25 Hastings Comm & Enter L J 359, 411–51 (2003).

[267] See 47 USC § 310(d). See also notes 255–56 and accompanying text.

[268] Syria in particular is known for taking an aggressive approach to Internet issues; for example, local Internet for the entire country was shut down in 2012. See Iain Thomson, *Syria Cuts Off Internet and Mobile Communications* (The Register, Nov 29, 2012), archived at http://perma.cc/SLR5-AMGZ.

[269] See A. Michael Froomkin, *Form and Substance in Cyberspace*, 6 J Small & Emerging Bus L 93, 109–10 (2002).

responsibility in ICANN. The license model is only as good as the policies ICANN chooses to pursue through its terms and restrictions on TLD administration, and those policies will be influenced by ICANN's governance structure. On the other hand, a strong property model that recognizes more rights in TLD registrars might be less subject to potential institutional decline on the part of ICANN and more amenable to international involvement. Because ICANN is incorporated in the United States, it may continue to find itself dragged into court to defend cases like *Stern*.

Although the license model is the most accurate description of current practice both within the legal system and in extralegal transactions, courts and policy makers today have a choice. ICANN and the various TLDs it controls through the root zone file are subject to US jurisdiction to the extent that courts or legislators wish them to be. Deciding which approach is normatively preferable ultimately comes down to how much the worries exemplified in *Stern*—that is, about Internet stability and splitting the root—matter compared to worries about potential dysfunction within ICANN.[270] This Comment opts for the license model not simply out of a commitment to descriptive accuracy within the law but also as a proactive choice to protect Internet stability.

CONCLUSION

The future of the DNS is still in flux. With the impending transfer of the root zone file away from US-government control, potential for a reorganization or rethinking of TLD ownership is high. Because TLDs undergird and enable the smooth functioning of the Internet as a whole, settling on a coherent and clear theory of TLD ownership has enormous implications.

None of the theories recognized by US courts seems wholly able to account for the normative considerations presented by TLDs. Some hybrid solution of the abstract-property theory and the service theory might avoid the worst outcomes: TLDs might be seen as property in some areas of law and not others. However, this solution is unwieldy and unpredictable, and it would require the determination of TLDs' property status to be made

[270] It may be that no single body, including ICANN, is fully trustworthy as a gatekeeper for the DNS—in which case agreements between the international community and ICANN that enforce some accountability, rather than ad hoc decisionmaking, would be necessary. See Sonbuchner, Note, 17 Minn J Intl L at 205 (cited in note 55).

afresh each time it is raised in litigation. Instead, courts should opt for a view of TLDs that draws comparisons to similar structures in licensing law: for example, broadcast licenses strongly resemble TLD-registry agreements and address the normative concerns of the DNS well. TLDs involve a complex interplay of public and private rights, and licensing law is adept at navigating this dynamic.