2021

Masters of Their Own Domains: Property Rights as a Bulwark Against DNS Censorship

Nicholas Nugent

MASTERS OF THEIR OWN DOMAINS: PROPERTY RIGHTS AS A BULWARK AGAINST DNS CENSORSHIP

NICHOLAS NUGENT*

It is increasingly becoming the practice of domain name system (DNS) intermediaries to seize domain names used by lawful websites for violating acceptable use policies related to offensive content or hate speech. Website hosting companies and social media platforms, entities that use but do not operate core Internet infrastructure, have long reserved and exercised their rights to gate their offerings, leaving booted speakers free to migrate to other providers. But registrants deprived of their domain names lack similar options to maintain their presence in cyberspace. The loss of a domain name inexorably results in the takedown of any website that uses the domain name, even if hosted elsewhere, and leaves a potentially invaluable asset essentially free for the taking by another. Proponents of Internet freedom have therefore argued that companies that operate foundational Internet infrastructure, such as the DNS, should play no role in policing content, no matter how deplorable, and that DNS censorship, once normalized, could easily spread to other minority groups and viewpoints.

Acknowledging that DNS intermediaries—the companies that offer domain names and make them operational on the Internet—are private actors whose actions are not subject to First Amendment constraints, critics of DNS censorship seem to tacitly concede that DNS intermediaries may take whatever actions are permitted under their terms of service, appealing instead to policy arguments or calls to enact new protective legislation. But I argue that registrants already possess the legal means to protect themselves from domain

* I would like to thank Christopher Yoo, Michael Froomkin, Milton Mueller, Ryan Calo, and Konstantinos Komaitis for helpful feedback and suggestions during the drafting process. Thanks also to Alexandra Bakalar for all the great research assistance. Original illustrations use icons made by Freepik and Kiranshastry from www.flaticon.com. The views expressed herein are entirely my own and do not necessarily reflect any policy positions held or endorsed by any current or former clients or employers.

name seizure through the property rights they acquire in their domain names.

Although the property status of domain names is by now fairly well established in the case law, scant attention has been paid to the precise nature of registrants' interests in that property. Making the case that registrants take title to their domain names upon registration, I argue that registrants may state valid claims under conversion and trespass to chattels when DNS intermediaries attempt to seize lawfully registered and operated domain names in the absence of court orders, despite the contractual rights such intermediaries purport to reserve to themselves. I further explore how federal law could supplement these existing common law protections by enshrining domain names as a new class of intellectual property.

INTRODUCTION

In August 2017, GoDaddy, the world's largest domain name registrar and website hosting provider, served notice to DAILYSTORMER.COM that the website had twenty-four hours to move its domain name to another registrar before the domain would be canceled.[1] Daily Stormer, GoDaddy alleged, had violated the latter's terms of service by hosting website content mocking the death of Heather Heyer, a woman killed in the course of protesting a white nationalist rally.[2] Within hours of moving to Google's domain management service, Google followed suit by first suspending[3] and then canceling Daily Stormer's domain name.[4]

In October 2018, GoDaddy issued a similar eviction notice to GAB.COM, the so-called "free speech Twitter,"[5] for hate speech

1. Daniel Van Boom & Claire Reilly, *Neo-Nazi Site The Daily Stormer Down After Losing Domain*, CNET (Aug. 14, 2017, 11:19 PM), https://www.cnet.com/news/neo-nazi-website-daily-stormer-to-lose-domain-name [https://perma.cc/DPW8-7VW9]; *see also Domain Name Registrar Stats*, DOMAINSTATE, https://www.domainstate.com/registrar-stats.html [https://perma.cc/Q3DN-VU92] (last visited Nov. 5, 2020) (for GoDaddy's share of global domain name and hosting market).

2. Bill Chappell, *Neo-Nazi Site Daily Stormer Is Banned By Google After Attempted Move From GoDaddy*, NPR (Aug. 14, 2017, 8:30 AM), https://www.npr.org/sections/thetwo-way/2017/08/14/543360434/white-supremacist-site-is-banned-by-go-daddy-after-virginia-rally [https://perma.cc/NZT9-EPST].

3. Michele Neylon, *DailyStormer Offline as Google Pulls Domain Registration*, INTERNETNEWS (Aug. 15, 2017), https://www.internetnews.me/2017/08/15/dailystormer-offline-google-pulls-domain-registration [https://perma.cc/HEY6-KMZB].

4. Jim Finkle, *Neo-Nazi Group Moves to 'Dark Web' After Website Goes Down*, REUTERS (Aug. 15, 2017, 7:42 AM), https://www.reuters.com/article/uk-virginia-protests-daily-stormer-idUKKCN1AV1I0 [https://perma.cc/4CWD-E6SJ].

5. Kassy Dillon, *Introducing 'Gab': Free Speech Twitter Alternative*, WASH. EXAMINER (Aug. 21, 2016, 11:07 AM), https://www.washingtonexaminer.com/red-alert-politics/introducing-gab-free-speech-twitter-alternative [https://perma.cc/N8UX-D9EG].

posted by users on the website.[6] When Gab proved unable to transfer its domain name to another registrar within twenty-four hours, GoDaddy suspended the domain, effectively taking the website down until another registrar was found.[7] One month later, DoMEn d.o.o., the company responsible for managing the .ME top-level domain, suspended INCELS.ME, a domain name used by a forum for "involuntary celibates," after the website failed to remove user content that promoted violence.[8] The domain name remained offline for more than a year thereafter.[9]

These actions were consistent with a broader trend in which domain name system (DNS) intermediaries, such as registrars and registry operators, have begun to take a more active role in policing website content through their control over Internet domain names.[10] This trend began with efforts by DNS intermediaries to combat online piracy and quickly expanded to other categories of illegal conduct, such as child pornography and "rogue" online pharmacies.[11] However, the new form of content regulation that brought down DAILYSTORMER.COM, GAB.COM, and INCELS.ME differed from previous campaigns by DNS intermediaries in one important respect: it concerned *legal* content. In all three cases, the basis for suspension was community speech found on the registrants' websites that, although certainly offensive, was fully protected under the First Amendment.

While some groups have cheered these developments and urged DNS intermediaries to play a stronger role in combating hate speech,[12] advocates of online freedom have argued that, unlike Internet service providers or social media networks, DNS

---

6. Catherine Shu, *Far-right Social Network Gab Goes Offline After GoDaddy Tells it to Find Another Domain Registrar*, TECHCRUNCH (Oct. 28, 2018, 11:28 PM), https://techcrunch.com/2018/10/28/far-right-social-network-gab-goes-offline-after-godaddy-tells-it-to-find-another-domain-registrar [https://perma.cc/R462-HSYT].

7. *Id.*

8. *The Suspension of Incels.me*, .ME (Nov. 20, 2018), https://domain.me/the-suspension-of-incels-me [https://perma.cc/4V2L-UALA]; Matt Binder, *Incels.me, A Major Hub for Hate Speech and Misogyny, Suspended by .ME registry*, MASHABLE (Nov. 20, 2018), https://mashable.com/article/incels-me-domain-suspended-by-registry [https://perma.cc/VT83-MJ85].

9. *Id.*

10. *See* Michael Kunzelman, *Online Registrar Threatens to Drop Anti-Immigration Website*, ABC NEWS (June 22, 2020, 3:16 PM), https://abcnews.go.com/US/wireStory/online-registrar-threatens-drop-anti-immigration-website-71391728 [https://perma.cc/9ZJT-KQNA] (describing Web.com's threats to suspend VDARE.COM for its anti-immigration views).

11. *See infra* Part II.A.

12. *See, e.g.*, *FAQs*, CHANGE THE TERMS, https://www.changetheterms.org/faqs [https://perma.cc/VG2E-5VR4] (last visited Oct. 18, 2020) (promoting the work of a coalition of civil rights groups to encourage technology companies to use their terms of service to curb "hateful activity," including, notably, companies that provide domain name services).

intermediaries do not host or transmit any content and therefore should play no role in policing speech that is external to their systems.[13] The latter fear that allowing private domain name companies to effectively boot entities from the Internet based on the expressive content of websites risks creating tools of censorship that could be leveraged in the future to suppress other viewpoints or causes.[14] Commentators have also noted with alarm the lack of due process protections that often accompany domain name takedowns, whether for legal or illegal conduct.[15]

But even assuming we want domain name companies to operate the DNS in a content-neutral manner—a goal I assume in this article—it might seem that little can be done to ensure that outcome. DNS intermediaries are private actors, and the Supreme Court has long held that the First Amendment does not protect speech from censorship by private actors, with limited exceptions that have not been extended to cyberspace.[16] And although the

13. *See, e.g.*, Jeremy Malcom, Cindy Cohn & Danny O'Brien, *Fighting Neo-Nazis and the Future of Free Expression*, ELECTRONIC FRONTIER FOUND. (Aug. 17, 2017), https://www.eff.org/deeplinks/2017/08/fighting-neo-nazis-future-free-expression [https://perma.cc/5KKV-WZQM] ("Companies that manage domain names, including GoDaddy and Google, should draw a hard line: they should not suspend or impair domain names based on the expressive content of websites or services.") [hereinafter Malcom et al., *Fighting Neo-Nazis*].

14. *Id.* ("[W]e must also recognize that on the Internet, any tactic used now to silence neo-Nazis will soon be used against others, including people whose opinions we agree with."); *see also* Michael C. Dorf, *Free Speech Issues Raised by Internet Companies Denying Service to Neo-Nazi Sites*, VERDICT (Aug. 23, 2017), https://verdict.justia.com/2017/08/23/free-speech-issues-raised-internet-companies-denying-service-neo-nazi-sites [https://perma.cc/H8CW-QDH6] (posing hypotheticals of other groups or causes that could be de-platformed by means of DNS takedown); Will Oremus, *GoDaddy Joins the Resistance*, SLATE (Aug. 16, 2017, 2:10 PM), https://slate.com/technology/2017/08/the-one-big-problem-with-godaddy-dropping-the-daily-stormer.html [https://perma.cc/SPW8-5BFU] ("Cutting off domain hosting is a potent weapon against the purveyors of objectionable content—and it could be double-edged.").

15. *See, e.g.*, Jeremy Malcolm & Mitch Stoltz, *How Threats Against Domain Names Are Used to Censor Content*, ELECTRONIC FRONTIER FOUND. (July 27, 2017), https://www.eff.org/deeplinks/2017/07/how-threats-against-domain-names-used-censor-content [https://perma.cc/9AA7-3G85] (noting the lack of due process protections for registrants whose domain names are taken down for service violations) [hereinafter Malcolm & Stoltz, *Threats*]; Annemarie Bridy, *Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation*, 74 WASH. & LEE L. REV. 1345, 1385 (2017) ("Lack of transparency and due process in such programs will make them inherently vulnerable to inconsistency, mistake, and abuse and could transform the DNS into a potent tool for suppressing disfavored speech.") [hereinafter Bridy, *Notice and Takedown*].

16. *See* Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 699, 702 (2010) ("Under current law, the First Amendment only restricts the actions of state actors and does not restrict the actions of private actors.") and ("[F]ree speech considerations favor preserving intermediaries' editorial discretion unless the relevant technologies fall

United States used to exercise oversight over the Internet Corporation for Assigned Names and Numbers (ICANN)—the non-profit corporation that sets policy for the DNS—that power was relinquished in 2016 when the United States permitted ICANN to transition to a global multi-stakeholder governance model.[17] DNS intermediaries thus have wide latitude, it would seem, to impose content-based restrictions on domain name registrants through their terms of service and to enforce those terms through the self-help remedies of domain name suspension, cancellation, and transfer.

In this article, I argue that one potential bulwark against content regulation by DNS intermediaries—one that has been largely overlooked—is registrants' property rights in their domain names. Although once the subject of debate between different lines of cases, both federal and state courts in the United States have largely settled on the proposition that domain names are a form of personal property and that a registrant may state a claim for conversion against an entity that unlawfully interferes with that property.[18] Thus far, such conversion claims have been brought almost exclusively in situations where one registrant manages to appropriate another registrant's valuable domain name in order to commercialize the name for its own purposes.[19] In other words, the goals of both plaintiff and defendant have been the same: to *use* the domain name for a website. However, if we take the property nature of domain names seriously, we see that similar conversion claims could be made by domain name owners against DNS intermediaries who suspend, cancel, or transfer domain names in the absence of court orders or similar legal processes. Consulting the closest available analogs in disparate areas of law such as repossession, bailment, and liquidated damages, I argue that such property rights may even suffice to override explicit contractual terms granting DNS intermediaries the right to seize domain names for breach of contract.

This article proceeds as follows. Part I presents a technical overview of the DNS with a particular view to separating core DNS services from non-core and value-added services that intermediaries might provide. Part II analyzes various provisions in DNS intermediary service contracts that purport to empower

---

within a narrow range of exceptions, all of which the Court has found to be inapplicable to the Internet.").

17. *See ICANN's Historical Relationship with the U.S. Government*, ICANN, https://www.icann.org/en/history/icann-usg [https://perma.cc/MH7S-SYQG] (last visited Oct. 18, 2020) (detailing the multi-year process by which the U.S. Department of Commerce turned control of ICANN over to a system of global stakeholders).

18. *See infra* Parts IV.A–C.

19. *See* Kremen v. Cohen, 337 F.3d 1024, 1035 (9th Cir. 2003).

DNS intermediaries to regulate content. It also describes ways, both systematic and *ad hoc*, in which DNS intermediaries have exercised that power. Part III traces the historical debate as to whether domain names should be classified as property versus mere contractual rights. It explains how the property view of domain names has become the consensus position and shows why this view is correct. It further analyzes the previously ignored issue of which party holds title to a registered domain name and concludes that only the registrant could legitimately be regarded as the owner. Finally, Part IV argues that a robust doctrine of domain names as property can be used to cabin intermediaries' private regulatory power. It explains how common law claims of conversion or trespass to chattels could be brought against DNS intermediaries who interfere with domain names in response to legal, or perhaps even illegal, web activity. But it notes the legal and practical limitations of such common law remedies and, therefore, explores additional potential options for strengthening property rights, such as through federal legislation that would recognize domain names as a new and distinct class of intellectual property.

I. TECHNICAL OVERVIEW OF THE DNS

Although many primers already exist that describe the structure and operation of the DNS, the arguments presented in this article turn on specific technical and historical nuances that are either absent from introductory descriptions or otherwise buried within advanced texts on the subject. Hence, in this Part, I aim to survey the DNS in a way that covers some of the more specialized details omitted by other summaries while remaining accessible to a generalist audience. Section A explains how users and computers use domain names in real time to locate content on the Internet. Section B describes the roles played by various intermediaries in that process.

A. IP Addresses and Domain Names

At the heart of nearly all modern Internet communication lies the mighty Internet Protocol (IP) address, a unique, 32-bit identifier represented as a string of up to twelve digits—for example, 93.184.216.34—that indicates the logical location of a device on the public Internet.[20] For a first computer (a client) to

20. This definition and the explanation that follows assume the use of IPv4 addresses which are still used by most Internet devices. Although a movement is under way to convert all public Internet traffic to the more flexible and capacious IPv6 standard, that development is not germane to this article and has no bearing on its

communicate with a second computer (a host), the client must append the host's IP address to any message it sends, and the host, in turn, must append the IP address of the client in any response. But twelve-digit strings are difficult for users to remember, and so the domain name system (DNS) was devised to make it easier for users to access resources on the Internet without having to remember IP addresses.[21]

Fundamentally, the concept behind the DNS is quite simple: create a list (a registry) that maps alphanumeric hostnames to IP addresses—e.g., "UCLA_server: 137.117.9.38"—then, when a user wishes to access an Internet resource, such as a website, she need only enter the hostname into her browser. The registry is consulted to find the IP address of the host (here, a web server), and then the user's computer uses the IP address to request the resource (here, a web page) from the host. As a result, the user no longer needs to know the IP address of any website to access it. She need only know the hostname, and the DNS and her computer will take care of the rest.

Building upon this basic concept, the architects of the early Internet designed the DNS with several important enhancements including top-level domains, authoritative registries, and caching. Starting with top-level domains, as the number of servers connected to a network increased, so did the risk of naming collisions, wherein two different entities seek to use the same hostname.[22] One solution to this problem was to create separate zones, also known as "domains," for hostnames based on the type or purpose of the host. Accordingly, in 1984, the Internet Engineering Task Force (IETF) published RFC 920, which proposed the creation of six "top-level domains" (TLDs), including COM (commercial), EDU (education), GOV (government), and ORG (a catch-all for other organizations).[23] The result was the modern "domain name" syntax that remains in use today, in which a top-level domain (e.g., COM) follows a second-level domain (e.g., MICROSOFT) with the two strings separated by a dot—hence, MICROSOFT.COM. This design permits two different entities to use the same hostname in

---

arguments. *See generally* Andy Patrizio, *IPv4 vs. IPv6: What's the Difference?* AVAST (May 8, 2020), https://www.avast.com/c-ipv4-vs-ipv6-addresses [https://perma.cc/7JUY-G9MW].

21. Frederick M. Abbott, *On the Duality of Internet Domain Names: Propertization and Its Discontents*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 1, 3 (2013) ("[T]he domain name is the 'human friendly' way of solving the memory and data entry problem.").

22. NAT'L RESEARCH COUNCIL, SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION 41 (2005).

23. *See* J. Postel & J. Reynolds, *Request for Comments 920: Domain Requirements*, INTERNET ENGINEERING TASK FORCE 7–8 (Oct. 1984), https://tools.ietf.org/html/rfc920 [https://perma.cc/6VJS-4Q32].

different domains—e.g., FMC.COM (Ford Motor Company) vs. FMC.EDU (Fine Mortuary College)—without any conflict.

Next, for a name-to-address mapping to be effective, it must be globally consistent. It will not do for some clients to map FACEBOOK.COM to one set of IP addresses while other clients map it to a different set. Moreover, if Facebook elected to change an IP address, some mechanism must exist to inform any clients using the old IP address to switch over to the new address. Hence, at the core of the modern DNS is the concept of authoritative registries. For each top-level domain, a single entity known as a "registry operator" maintains an authoritative zone file that contains information for all domain names registered within the top-level domain.[24] For example, Verisign, Inc., which operates the .COM top-level domain, maintains the authoritative zone file for all .COM domain names.[25] Any computer may therefore determine the IP address for any .COM domain name by sending a DNS query to Verisign's nameservers.

But because it would strain a registry operator's servers to respond to a DNS query every time a computer uses a domain name, the DNS makes extensive use of caching. When a nameserver responds to a DNS query with authoritative IP address information about a domain name, its response also includes a "time-to-live" (TTL) value, which can range from seconds to days, indicating how long the information should be regarded as valid. Any computers receiving the response are expected to store (cache) the information in memory and use it for all future communications involving the domain name, rather than querying the registry operator each time, until the TTL expires, at which time the DNS information is deleted from cache."

24. *See* GlobalSantaFe Corp. v. Globalsantafe.com, 250 F.Supp.2d 610, 618–19 (E.D. Va. 2003); NAT'L RESEARCH COUNCIL, *supra* note 22 at 120–21; MARK E. JEFTOVIC, MANAGING MISSION-CRITICAL DOMAINS AND DNS 32 (2018). Registry operators are sometimes referred to simply as "registries." To avoid any confusion with the registry databases maintained by registry operators, this article uses the long form "registry operators" throughout.

25. *See Root Zone Database*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/domains/root/db [https://perma.cc/KUN5-H7UD] (last visited Oct. 18, 2020).

The following diagram illustrates these concepts in the context of an actual DNS query.[26] Although all steps depicted in Fig. 1 are relevant to how domain names are used to access web content, the reader is directed to pay close attention to the description of Steps 4–5 and 9–10 which will prove central to certain arguments against DNS censorship.

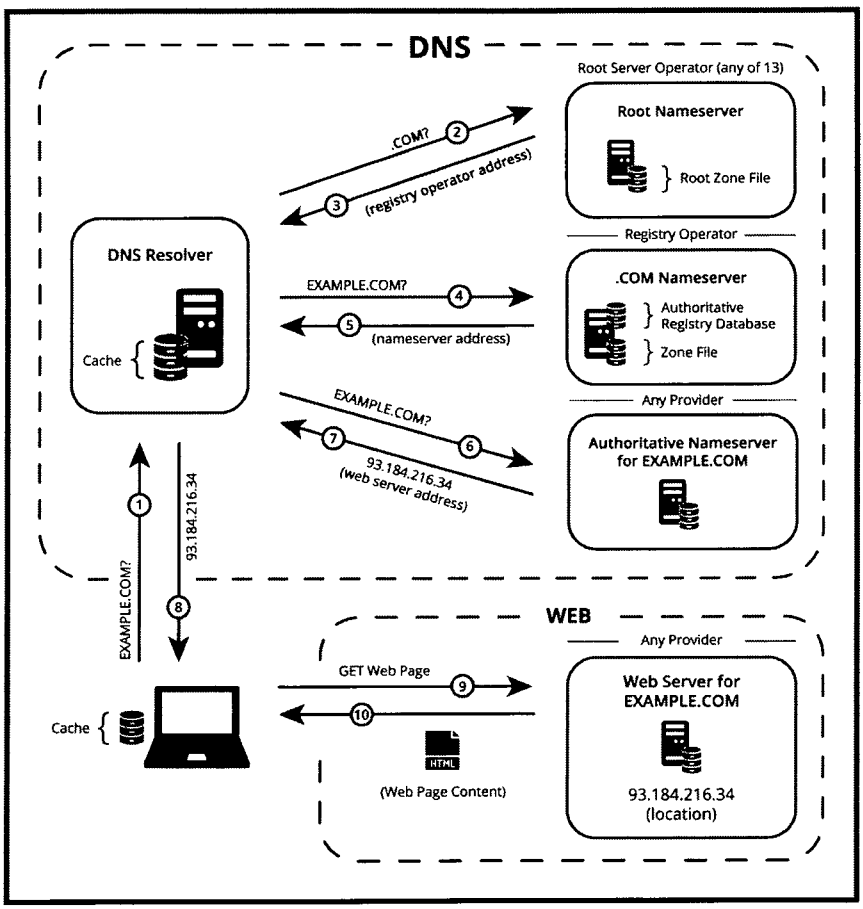


FIGURE 1

The process begins when a client needs to communicate with a host but has only the host's domain name. Although the client and host may be any two computers on the Internet and the communication may occur in the context of any type of Internet activity, whether or not involving a human participant, for

26. The savvy DNS practitioner will observe that the process has been simplified and that certain intermediate steps have been omitted for ease of discussion.

purposes of this illustration, I use the familiar scenario in which an end user attempts to visit a website by typing a domain name—here, EXAMPLE.COM—into his browser. The end user's computer first consults its local cache. Has the user visited EXAMPLE.COM recently such that its IP address is already stored locally on the computer? If not, the computer sends a DNS query to a DNS Resolver (Step 1), which is typically provided by the user's Internet service provider but may be operated by any service provider or by the user himself.

The DNS resolver then consults its own cache. Has the DNS resolver received a DNS query for EXAMPLE.COM from another user or computer recently such that its IP address is already cached in memory? To illustrate the entire end-to-end flow, we will assume that the cache in the DNS Resolver is empty[27] and that the full DNS resolution process must play out. Without any information about the requested name, the DNS Resolver looks first to the most basic component of the domain name: its top-level domain (here, .COM). To find a server that can provide authoritative information about .COM names, the DNS Resolver sends its own query to a root nameserver which is operated by an entity called a root server operator (Step 2). The root server operator maintains an authoritative "root zone file" that contains the name and IP address of the registry operator for each top-level domain.[28] The root nameserver responds to the query by sending back the IP address for the .COM nameserver (Step 3).

Using the IP address returned by the root nameserver, the DNS resolver sends a DNS query for EXAMPLE.COM to the .COM nameserver (Step 4), which is operated by the .COM registry operator. Just as a root server operator maintains an authoritative root zone file containing information about all top-level domains in the root (i.e., the Internet), the registry operator for a given top-level domain maintains an authoritative zone file containing information about all second-level domains (i.e., the "EXAMPLE" in EXAMPLE.COM) in the top-level domain. Accordingly, in response to the query from the DNS resolver, the .COM nameserver checks the .COM zone file to see if a record exists for EXAMPLE.COM. If so, it responds with the information in that domain name record.

---

27. While the cache may be empty, a DNS resolver should nonetheless be pre-programmed with the names and IP addresses of the thirteen root servers. Without this *a priori* information, authoritative DNS resolution is not possible. DANIEL KARRENBERG, THE INTERNET DOMAIN NAME SYSTEM EXPLAINED FOR NON-EXPERTS 4–5 (2017), https://www.internetsociety.org/wp-content/uploads/2017/09/The-Internet-Domain-Name-System-Explained-for-Non-Experts-ENGLISH.pdf [https://perma.cc/76MQ-3E9V].

28. NAT'L RESEARCH COUNCIL, *supra* note 22, at 96–97.

In theory, the DNS could have been designed so that the zone file for a top-level domain stores the actual IP address for each domain name in the top-level domain. For example, if the website associated with EXAMPLE.COM is hosted at 93.184.216.34, the .COM nameserver could just respond to DNS queries for EXAMPLE.COM by returning that IP address. In practice, however, rather than storing the actual IP address of the domain name host, the zone file stores the IP address of a separate computer called an authoritative nameserver. An authoritative nameserver is a server that is ultimately responsible for providing the IP address associated with a domain name. The domain name owner can choose any available service provider to operate an authoritative nameserver for his domain name or could even operate the nameserver himself.[29]

Thus, in this example, the .COM registry operator responds to the query by returning the IP address of the authoritative nameserver for EXAMPLE.COM (Step 5). Next, using the IP address returned by the .COM registry operator, the DNS resolver sends a DNS query to the authoritative nameserver for EXAMPLE.COM (Step 6). At long last, the authoritative nameserver responds with the actual IP address at which the domain name is hosted (Step 7). At this point, the website address is known. The DNS query, and the domain name associated with it, can be said to have "resolved." The DNS resolver updates its cache and returns the IP address to the user's computer (Step 8).[30] Finally, the user's computer sends a request[31] for a web page to the web server hosted at the IP address associated with the domain name (Step 9), and the web server responds by sending the content contained in the requested web page (Step 10). The user has, thus, successfully accessed a website despite knowing only its domain name mnemonic.

Two important observations can be gleaned from this architecture. First, the process is inherently authoritative and

29. The rationale for storing the IP address of an authoritative nameserver in the zone file, rather than the IP address of the host, is that the domain name owner can change the IP address of the host at any time by simply updating the authoritative nameserver instead of requiring the registry operator to change the zone file. Otherwise, in a sea of millions of domain names within a top-level domain with hosts constantly shifting from one IP address to another, a registry operator would potentially need to update the zone file for the top-level domain many times per second.

30. The user's computer may also update its own cache to avoid the need to request the IP address again until the time-to-live (specified in the DNS record returned by the authoritative nameserver) expires.

31. In this case, a hypertext transfer protocol (HTTP) request.

centralized.[32] A single, authoritative zone file exists for each top-level domain, and a single entity—the registry operator—maintains that zone file and responds to queries for information about any domain names within the top-level domain (Steps 4 and 5). If the registry operator fails to resolve queries for a given domain name for any reason, Internet traffic that relies on the domain name will function only for as long as the IP address of the domain name host remains in cache somewhere in the DNS query chain (typically, less than 24 hours).[33] Thereafter, any network communications that rely on the domain name will fail. If the domain name is associated with a website, the website will be effectively inaccessible. Although the website will continue to be reachable through its IP address, users who do not know that IP address (the vast majority of users) will not be able to access the website.[34] As explained *infra*,[35] it is this central control over the DNS resolution process that provides registry operators with unique control over the accessibility of website content and thus makes DNS censorship possible.

Second, no content ever flows through the DNS itself, whether website, email, video, chat, or other content.[36] The DNS exists only to answer a simple question—what IP address is associated with a given domain name? Once the requesting computer receives the answer to that question, it communicates directly with the host (using the IP address) through an Internet service provider and not through any DNS servers. The servers involved in resolving a DNS query (Steps 1-8) have no visibility into what the requesting computer does with the returned IP address (Steps 9 and 10)—much less the content provided by the host located at the address.

---

32. Although the DNS is often rightly described as a decentralized system, it is nonetheless centralized insofar as only one entity—the registry operator for the relevant top-level domain—maintains the zone file for a given top-level domain and responds to DNS queries for domain names within the zone file.

33. *See* Jeff Petters, *What is DNS TTL + Best Practices*, VARONIS: INSIDE OUT SECURITY BLOG https://www.varonis.com/blog/dns-ttl/ [https://perma.cc/92L5-329R] (last updated July 14, 2020) (calculating the average TTL value of the top 500 sites at 6,468 seconds or just under two hours).

34. *See* GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 620 n.31 (E.D. Va. 2003) ("[S]ince use of domain names is so ubiquitous, few if any users will know the relevant IP address.").

35. *See infra* Part II.A.

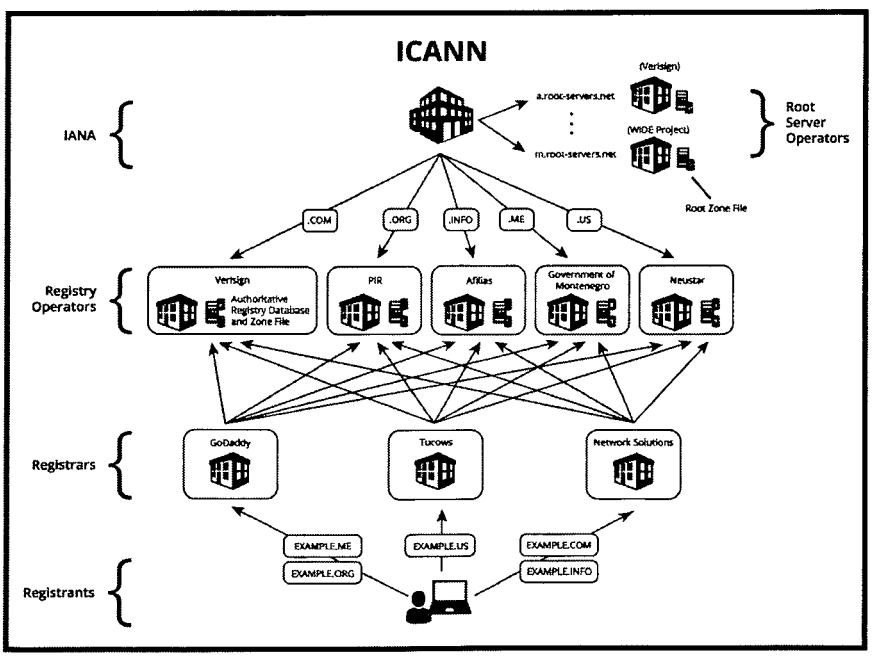
36. *See* Malcom et al., *Fighting Neo-Nazis*, *supra* note 13 ("Domain name companies also have little claim to be publishers, or speakers in their own right, with respect to the contents of websites. Like the suppliers of ink or electrical power to a pamphleteer, the companies that sponsor domain name registrations have no direct connection to Internet content. Domain name registrars have even less connection to speech than a conduit provider such as an ISP, as the contents of a website or service never touch the registrar's systems.").

In this manner, the DNS has been analogized to a phonebook.[37] It is used to look up numbers associated with the names of persons or organizations but plays no role in the activities performed by those listed persons or organizations. As further described *infra*,[38] the fact that web content is wholly external to the DNS provides one of the strongest policy arguments against DNS censorship.

B. DNS Intermediaries

Entities that necessarily participate in the operation or management of the DNS (for purposes of this article, "DNS intermediaries") generally fall into one or more of the following categories: Internet Assigned Numbers Authority (IANA), root server operators, registry operators, and registrars. The following diagram depicts the relationship between the various DNS intermediaries.

FIGURE 2



37. *See, e.g.*, XUEBIAO YUCHI, GUANGGANG GENG, ZHIWEI YAN & XIAODONG LEE, CHINA INTERNET NETWORK INFORMATION CENTER, TOWARDS TACKLING PRIVACY DISCLOSURE ISSUES IN DOMAIN NAME SERVICE 813 (describing the DNS as "the global Internet's phonebook"); Becky Hogge, *The Great Phonebook in the Sky*, NEW STATESMAN (Feb. 7, 2008) https://www.newstatesman.com/scitech/2008/02/web-users-beards-sandals-dns [https://perma.cc/8PF7-W8RV] ("Think of it as a great big telephone directory in the sky.").

38. *See infra* Part II.B.

As depicted, each top-level domain is managed by a single registry operator, be it a for-profit or non-profit corporation, a state-controlled entity, or a government agency.[39] Although only five top-level domains are depicted in Fig. 2, and only seven top-level domains existed when the DNS was first implemented in 1985, website operators may now choose from among 1,587 top-level domains when registering a domain name.[40] The vast majority of top-level domains (1,242 as of this article) are classified as generic top-level domains (gTLDs)[41] meaning that any person or entity may theoretically register a domain name within the TLD for any purpose. Examples of gTLDs include the .COM, .ORG, and .NET legacy TLDs as well as newer strings, such as .BOOK, .FUN, and .XYZ. Set against these permissive gTLDs are generic-restricted and certain sponsored top-level domains which limit registration to certain classes of organizations or individuals.[42] Examples include .BIZ (reserved for business entities), .EDU (accredited post-secondary institutions), .JOBS (human resources managers), and .XXX (adult entertainment). In some cases, a registry operator may limit registration within a branded top-level domain (e.g., .BMW) to itself and its affiliates—a "closed TLD."[43]

The remaining top-level domains[44] (315 as of this article) are classified as country code top-level domains (ccTLDs), predominantly two-character strings that map to a distinct country, sovereign state, or dependent territory.[45] Examples include .US (United States), .CN (China), and .NP (Nepal).[46] Country code top-level domains are typically delegated to the government of the country or territory to which they refer or to a private entity within

39. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 129.

40. *See Root Zone Database*, *supra* note 25 (listing each operational top-level domain).

41. *Id.*

42. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 114 (comparing the different categories of generic top-level domains, including sponsored-restrictive, sponsored-unrestrictive, unsponsored-restrictive, and unsponsored-unrestrictive).

43. *See* Paul Sawers, *Google Domains Moves to a '.Google' domain*, VENTUREBEAT (Mar. 30, 2016, 4:23 AM), https://venturebeat.com/2016/03/30/google-domains-dot-google/ [https://perma.cc/6LTJ-UCGA].

44. In this explanation, I have excluded the remaining infrastructure and test categories, which consist of fifteen top-level domains used only for technical and test purposes and not in conjunction with any meaningful websites. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 114–20.

45. *Id.* at 113; JEFTOVIC, *supra* note 24, at 33–34.

46. *Country Domains: A Comprehensive ccTLD List*, IONOS, https://www.ionos.com/digitalguide/domains/domain-extensions/cctlds-a-list-of-every-country-domain/ [https://perma.cc/9VE7-Z8W6] (last visited Oct. 18, 2020).

the country or territory,[47] although technical operations may be outsourced to another entity, whether domestic or foreign.[48]

Country code top-level domain managers may set their own policies concerning who may register domain names within their top-level domains.[49] In some cases, a country will impose strict registration criteria (e.g., .JP domain names are limited to individuals and corporations located in Japan).[50] In other cases, a country will allow any organization or individual to register within its ccTLD, resulting in an additional class of *de facto* generic top-level domains that may be popular because of their similarity to English words or acronyms—e.g., .ME (Montenegro), .TV (Tuvalu)—or because they can be used as "domain hacks" to spell other words—e.g., INSTAGR.AM (Armenia), YOUTU.BE (Belgium).[51]

Although an entity may manage more than one top-level domain, each top-level domain is delegated to only a single registry operator.[52] As described *supra*, by vesting a single entity with the

---

47. NAT'L RESEARCH COUNCIL, *supra* note 22, at 10; *Common Questions on Delegating and Transferring Country-Code Top-Level Domains (ccTLDs)*, INTERNET ASSIGNED NUMBERS AUTHORITY https://www.iana.org/help/cctld-delegation-answers [https://perma.cc/93Q5-M9Q5] (last visited Oct. 18, 2020) ("For each ccTLD, at a minimum both the manager and the administrative contact must be resident in the country to which the domain is designated. This means they are accountable to the local community and subject to local law.").

48. For example, Verisign, a U.S. company, currently operates the .CC (Cocos Island) and .TV (Tuvalu) ccTLDs on behalf of the local delegated managers. *See Get Creative With A .cc Domain Name*, VERISIGN, https://www.verisign.com/en_US/domain-names/cc-domain-names/index.xhtml [https://perma.cc/8P8N-YLCK] (last visited Oct. 18, 2020); *A .tv Domain Name Is Where the World Turns for Entertainment*, VERISIGN, https://www.verisign.com/en_US/domain-names/tv-domain-names/index.xhtml [https://perma.cc/4KB9-TW98] (last visited Oct. 18, 2020).

49. *See About ccTLD Compliance*, ICANN, https://www.icann.org/resources/pages/cctld-2012-02-25-en [https://perma.cc/M38H-4CE4] (last visited Oct. 18, 2020) ("The ccTLD policies regarding registration, accreditation of registrars and Whois are managed according to the relevant oversight and governance mechanisms within the country, with no role for ICANN's Compliance department in these areas.").

50. *About .jp domains*, GODADDY, https://www.godaddy.com/help/about-jp-domains-20219 [https://perma.cc/Q5HY-726G] (last visited Oct. 18, 2020); *see also About ccTLDs (Country-Code Domain Names)*, GODADDY https://www.godaddy.com/help/about-cctlds-country-code-domain-names-6243 [https://perma.cc/HK7K-GTJN] (last visited Oct. 18, 2020) (providing specific requirements and considerations for various ccTLDs).

51. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 116–17 (noting that the distinction between generic top-level domains and country code top-level domains has significantly eroded).

52. *Id.* at 129 ("There is always one, and only one, registry for a given TLD, but, as noted above, an organization can be the registry operator for more than one TLD."). For example, Binky Moon, LLC d/b/a "Donuts" manages nearly 200 different top-level domains, including .COMPANY, .GIFTS, and .TOYS. *See also Root Zone Database*, *supra* note 25.

responsibility of maintaining the authoritative zone file for a top-level domain, the risk of naming collisions is effectively eliminated.[53] The registry operator not only maintains the zone file for its top-level domain but also operates the nameserver for the top-level domain, responding to DNS queries for domain names registered therein (Steps 4 and 5 in Fig. 1).

In addition to the zone file, the registry operator maintains an authoritative registry database for the top-level domain. The registry database lists authoritative information about each domain name that has been registered within the top-level domain including, typically, the name and contact information of the person or business who registered the domain name, the registration creation and expiration date, and the domain status.[54] Whereas the zone file maintained by the registry operator functions like a phonebook, listing addresses associated with names. The registry database can best be analogized to a land registry maintained by a county title office or similar administrator. Because only one entity can be listed as the holder of a domain name, the registry database, which is publicly accessible through a WHOIS service, operated by registrars and registry operators, serves to put the world on notice of which parties claim exclusive rights to which domain names.[55] Registering a domain name, therefore, is fundamentally a matter of recording a person's or organization's interest in the domain name within the authoritative registry database for the associated top-level domain. As we'll see,[56] the distinction between recordation in the authoritative registry database and the answering of DNS queries from the zone file will prove important when it comes to separating the property status of domain names from certain domain-related services provided by DNS intermediaries.

---

53. *See supra* Part I.A.

54. *Registry Agreement: Appendix C*, ICANN, §§ C2.1, C5, (June 6, 2003) https://www.icann.org/resources/unthemed-pages/registry-agmt-appc-redlined-2003-06-06-en [https://perma.cc/6Q8Q-E5CP] ("[T]he registry database [is] the authoritative source of domain names and their associated hosts (name servers)."); GlobalSantaFe Corp., v. Globalsantafe.com, 250 F. Supp. 2d 610, 619 (E.D. Va. 2003) ("The registry . . . maintain[s] and operat[es] the unified Registry Database, which contains all domain names registered by all registrants and registrars in a given top level domain . . . .").

55. *See About WHOIS*, ICANN https://whois.icann.org/en/about-whois [https://perma.cc/XCU4-A5GG] (last visited Oct. 18, 2020). Although the .COM and .NET legacy gTLDs operate in a "thin registry" model in which information about the registrar, rather than the registrant, is stored in the registry database, information about the registrant is nonetheless accessible through the WHOIS service, which queries both the registry operator's and the registrar's databases to identify the end registrant. *See What Are Thick and Thin Entries?*, ICANN, https://whois.icann.org/en/what-are-thick-and-thin-entries [https://perma.cc/CJE8-NPQG] (last visited Oct. 18, 2020). In any event, an effort is under way to convert .COM and .NET to "thick registries." *Thick WHOIS*, ICANN (May 7, 2019), https://www.icann.org/resources/pages/thick-whois-2016-06-27-en [https://perma.cc/F3P2-QJXE].

56. *See infra* Part III.D.3.

Although registry operators maintain the authoritative registry databases for the top-level domains they manage, they typically do not offer domain name registration services directly to the public, at least for generic top-level domains.[57] Instead, when a person wishes to register a domain name, he engages the services of a domain name registrar, in most cases, through the registrar's self-service online registration system. For example, and as depicted in Fig. 2, a customer who wishes to register the domain name EXAMPLE.INFO might visit the website of a registrar, such as Network Solutions, Inc. The registrar then queries the authoritative registry database maintained by the registry operator responsible for the .INFO top-level domain (currently, Afilias Ltd.) to determine whether the domain name is available. If so, the customer pays the registrar-prescribed fee (the "registration fee"),[58] the registrar transmits the customer's information to the registry operator, and the registry operator creates a record in the registry database associating the domain name with the customer information so provided. At this point, the customer becomes the sole holder of the domain name and is deemed the "registrant." In addition, if the registrant wishes to make the domain name operational, he provides the registrar with the name and address of authoritative nameservers for his domain name, which the registrar forwards to the registry operator and the registry operator records in the zone file.

Registrars typically contract with multiple registry operators in order to be able to offer domain names across multiple top-level domains. Registry operators are likewise required to allow any accredited registrar to sell domain names within their top-level domains.[59] As a result, a customer who desires to register a domain name may choose from among thousands of different registrars.[60] Moreover, after registering a domain name through one registrar,

57. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 135–37 (chronicling the development of separate registry and registrar functions and entities).

58. As of this article, registration fees generally range from $2 to $20. Maxym Martineau, *How much does a domain name cost?*, GODADDY (July, 8, 2019), https://www.godaddy.com/garage/how-much-domain-name-cost/ [https://perma.cc/FR8J-Z8P8].

59. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 136 ("Under the terms of their agreements with ICANN, gTLD registries are required to permit registrars to provide Internet domain name registration services within their top-level domains.").

60. *See generally* ICANN, DESCRIPTIONS AND CONTACT INFORMATION FOR ICANN-ACCREDITED REGISTRARS, https://www.icann.org/registrar-reports/accredited-list.html [https://perma.cc/3N6P-AQQA] (last visited Oct. 18, 2020).

a registrant may later transfer his registration to another registrar.[61]

Domain names may be registered in one-year increments, up to a maximum registration term of ten years.[62] At any time during the registration term, a registrant may renew his registration by paying the prescribed renewal fee for a renewal term of one to ten years, provided that the total remaining registration term does not exceed ten years. In this manner, a registrant can maintain exclusive rights to his domain name indefinitely as long as he continues to renew the domain and pay the required renewal fees before his current registration term expires. If a registrant fails to renew his domain name before the registration term expires, a series of grace periods apply during which he may still renew the name subject to additional fees.[63] Once all grace periods have been exhausted, the registration is deleted, the domain name reverts to unregistered status, and any customer may register the name on a first-come basis.[64]

Importantly, upon expiration, control of the domain name reverts back to the registry operator and not to the registrar whom the registrant used to register the name.[65] Accordingly, just as when the domain name was originally registered, a new registrant may register it through any accredited registrar.[66] The original registrar can lay no greater claim to the domain name than any other registrar. If the registrar wishes to possess the now-expired domain name for its own purposes, it must register the domain name just like any other customer. And, despite knowing when an un-renewed domain name will expire, even the original registrar may not be the favorite to win the registration race. "Drop-catchers," a special class of professional domain name investors

61. *See Transfer Policy*, ICANN (June 1, 2016), https://www.icann.org/resources/pages/transfer-policy-2016-06-01-en [https://perma.cc/X336-8GHH] (providing registrants with the general right to transfer domain names between registrars).

62. *FAQs*, ICANN https://www.icann.org/resources/pages/faqs-2014-01-21-en [https://perma.cc/7RJY-D4UZ] (last visited Oct. 18, 2020) ("Each registrar has the flexibility to offer initial and renewal [registrations] in one-year increments, provided that the maximum remaining unexpired term shall not exceed ten years.").

63. JEFTOVIC, *supra* note 24, at 22–26.

64. *Id.* at 25–26.

65. *See id.* (explaining that final expiration of a domain name registration will result in deletion of the registration record from the authoritative registry database, which record would include any authoritative association between the domain name and the sponsoring registrar).

66. *See AGP Limits Policy and Draft Implementation Plan*, ICANN, https://www.icann.org/resources/pages/agp-draft-2008-10-20-en [https://perma.cc/UZ9Q-MHZD] (last visited Oct. 18, 2020) ("Once a domain name is deleted by the registry at this stage, it is immediately available for registration by any registrant through any registrar.").

("domainers"), employ sophisticated, automated systems to monitor high-value domain names that are scheduled for expiration and attempt to register them before any other entity.[67] As a result, valuable domain names are often snatched up by drop-catchers within seconds of their expiration.[68] As will be shown,[69] limited registration periods and control over expired domain names will prove relevant to the issue of which party may claim title to registered domain names.

Atop this organizational scheme sits the IANA. By itself, IANA is not an entity but a function (or set of functions), and the entity who performs the IANA function is responsible for coordinating the delegation of top-level domains and the allocation of IP addresses.[70] Since 2000, ICANN, a non-profit corporation headquartered in California, has performed the IANA function.[71] But prior to 2000, the function was performed by universities and, in its earliest incarnation, by a single individual, John Postel.[72] In performing the IANA function, ICANN is responsible for delegating each top-level domain to a registry operator, which it does pursuant to registry agreements typically lasting ten years.[73] Absent breach, a registry agreement may automatically renew for an additional ten-year period.[74] However, such a presumptive right to renewal was not always guaranteed to registry operators. Early registry agreements, such as ICANN's delegation of .COM to VeriSign and .ORG to Network Solutions, provided no presumptive right to

67. *See generally* NAJMEH MIRAMIRKHANI, TIMOTHY BARRON, MICHAEL FERDMAN & NICK NIKIFORAKIS, PANNING FOR GOLD.COM: UNDERSTANDING THE DYNAMICS OF DOMAIN DROPCATCHING, 2018 IW3C2 (INTERNATIONAL WORLD WIDE WEB CONFERENCE COMMITTEE, 2018).

68. *See* JEFTOVIC, *supra* note 24, at 25 ("If the [expired] domain has any marginal value . . ., then the 'drop-catchers' will now converge and the domain will be reregistered within a few milliseconds.").

69. *See infra* Part III.E.3.

70. *See About Us*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/about [https://perma.cc/SF57-YZY2] (last visited Oct. 18, 2019) (describing the IANA functions).

71. JOEL SNYDER, KONSTANTINOS KOMAITIS & ANDREI ROBACHEVSKY, THE HISTORY OF IANA: AN EXTENDED TIMELINE WITH CITATIONS AND COMMENTARY, INTERNET SOCIETY 5 (Jan. 2017), https://www.internetsociety.org/wp-content/uploads/2016/05/IANA_Timeline_20170117.pdf [https://perma.cc/EM4E-UB36].

72. *Id.* at 2–5.

73. *Base Registry Agreement*, ICANN, § 4.1 https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm [https://perma.cc/9T4W-4W8V] (last visited Oct. 18, 2020) [hereinafter *Base Registry Agreement*, ICANN].

74. *Id.* at § 4.2.

renewal. And ICANN was free to re-delegate such top-level domains to other parties upon expiration of the registry agreements.[75]

In addition to setting policy for the DNS through a global stakeholder process, the IANA function vests ICANN with responsibility for allocating IP address blocks to network operators around the world.[76] ICANN also oversees the Root Server System, a set of thirteen different root zone servers (lettered 'a' through 'm'), each of which hosts a copy of the root zone file and responds to DNS queries for the IP addresses of top-level domain nameservers (Steps 2 and 3 of Fig. 1).[77]

Notably, among these four categories of DNS intermediaries, only registry operators and root server operators necessarily participate in the resolution of domain names. As depicted in Fig. 1, when a query is made to resolve a domain name, in the absence of any temporarily cached information, the query is ultimately routed to a root server operator, then to the registry operator, and then to an authoritative nameserver for the domain name. Because it is impossible, under the current configuration of the DNS, for an un-cached DNS query to resolve if these functions are not performed, I refer to them as "core DNS services."

By contrast, at no point is it necessary for the registrar or ICANN to participate in the resolution of any domain name. Instead, the registrar's role is largely limited to registering and renewing domain names on the registrant's behalf, sending reminders when the domain name is approaching expiration (if applicable), and allowing the registrant to update aspects of the registration, such as contact information, nameserver delegation, and security parameters.[78] Registrars perform most or all of these functions through the registry operator's automated system.[79] In any event, none of these functions must be performed on a continual, real-time basis for a domain name to remain operational. Because registrars play no part in resolving DNS queries for

75. *See ICANN-NSI Registry Agreement*, ICANN, § 23 (Sept. 28, 1999), https://archive.icann.org/en/nsi/nsi-registry-agreement.htm [https://perma.cc/B42W-FCTK] (providing no presumptive right to renewal after eight years); *See also .org Registry Agreement*, ICANN, § 5.1 (May 25, 2001), https://www.icann.org/resources/unthemed-pages/registry-agmt-org-2001-05-25-en [https://perma.cc/Z5BA-27EP].

76. *See Number Resources*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/numbers [https://perma.cc/3A3C-ANWV] (last visited Oct. 18, 2020).

77. *See Root Servers*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/domains/root/servers [https://perma.cc/8XQC-F2GK] (last visited Oct. 18, 2020).

78. JEFTOVIC, *supra* note 24, at 37.

79. GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 619–20 (E.D. Va. 2003).

domain names, I refer to the administrative services they provide as "non-core DNS services."

To be sure, registrars frequently offer value-added services when customers register domain names, such as website hosting, email, or WHOIS privacy.[80] Indeed, such value-added services may provide the bulk of a registrar's net income, given the low profit margins involved in simply marking up domain name registration and renewal fees. And frequently, one such value-added service that a registrar offers when a customer registers a domain name is to allow the registrant to use the registrar's authoritative nameservers to resolve DNS queries for the domain name (Steps 6 and 7 in Fig. 1).[81] While authoritative name resolution *is* a core DNS service, a registrant is free to choose any available provider to operate authoritative nameservers for his domain and may even perform the function himself. Thus, after registering a domain name, the services of the sponsoring registrar are not strictly necessary for the name to remain operational.

Likewise, as the performer of the IANA function, ICANN's role is to set technical policy for the DNS, not to operate it.[82] Although ICANN delegates responsibility for managing top-level domains to registry operators, ICANN itself neither manages any top-level domain nor operates any top-level domain nameserver. And although ICANN operates one of the thirteen root zone servers, it does so only as one of thirteen mirrors and, thus, is not essential to the resolution of any DNS query. This distinction between core and non-core DNS services will become important when it comes to analyzing whether a given DNS intermediary should be able to suspend, cancel, or transfer a domain name in the course of terminating its relationship with a registrant.

II. DNS INTERMEDIARY POWER OVER CONTENT

DNS intermediaries lack direct control over Internet content. At any time, a user may visit a website by simply typing the IP address of a provider's web server into her browser and downloading the content provided by that server (Steps 9 and 10 of Fig. 1). These steps are wholly external to the DNS, and so

---

80. *Domain Name Industry*, ICANN, https://www.icann.org/resources/pages/domain-name-industry-2017-06-20-en [https://perma.cc/BW56-DAPR] (last visited Oct. 18, 2020) ("Many registrars also offer other services such as web hosting, privacy/proxy, website builder, etc.").

81. *See How Do I Find The DNS Provider Of My Domain?*, INTERMEDIA, https://kb.intermedia.net/article/1347 [https://perma.cc/7ASV-3FPT] (last visited Oct. 18, 2020) (explaining that DNS hosting for a domain name is commonly provided by the domain name registrar).

82. *See* Bridy, *Notice and Takedown*, *supra* note 15, at 1361 (describing ICANN's "narrow technical mandate").

registrars, registry operators, and even ICANN are powerless to interfere. But because IP addresses are not only difficult to remember but also constantly changing, DNS intermediaries can exert *de facto* control over website content through their control over the registration and resolution of domain names. In this part, I trace the history of that control, as intermediaries first tailored their agreements to prevent the DNS from becoming a tool of trademark infringement, then to disrupt criminality, and finally to police offensive, but legal, content.

A. Cybersquatting and Restrictions Against Illegal Content

In the early days of the DNS, domain names came with few, if any, strings attached. Even as late as 1994, one could register a domain name by simply emailing a request to Network Solutions, a private corporation under contract with the National Science Foundation (NSF) to manage several legacy top-level domains, including .COM and .ORG.[83] No registration fee was required and no contract governed the registration.[84] By the end of 1995, however, Network Solutions was receiving more than 20,000 registration requests per month—taxing its limited, NSF-funded resources and resulting in a five-week delay to register any name.[85] As a result, on September 14, 1995, the NSF authorized Network Solutions to begin charging a $50 fee to register new domain names and to retain such registration fees to offset operational costs.[86] Formal terms and conditions soon followed in the form of registration agreements that customers were required to accept in order to register domain names.

Early registration agreements were relatively simple, requiring the registrant to do little more than pay the required registration fee, provide accurate contact information, and submit

83. *See* Kremen v. Cohen, 337 F.3d 1024, 1026 (9th Cir. 2003) (describing the process by which Sex.com was registered in 1994). *See also* NAT'L RESEARCH COUNCIL, *supra* note 22, at 75–78 (explaining the contractual framework under which Network Solutions managed domain name registrations on behalf of NSF).

84. *See Kremen*, 337 F.3d at 1026–28; Caroline Bricteux, *Regulating Online Content through the Internet Architecture: The Case of ICANN's New gTLDs*, 7 J. INTELL. PROP. INFO. TECH. ELECTRONIC & COMM. L. 229, 232 (2016) ("At that time, registration of a SLD was subsidized by the NSF and free of charge for the end user.") [hereinafter Bricteux, *ICANN's New gTLDs*].

85. *The Internet Grows Up*, NSF (Sept. 14, 1995), http://www.nsf.gov/news/news_summ.jsp?cntn_id=100806 [https://perma.cc/DF78-5WR4].

86. *Id.*; Michael Brian Pope et al., *The Domain Name System: Past, Present, and Future*, 30 COMM. ASS'N FOR INFO. SYS. 329, 332 (2012).

to the registrar's dispute resolution policy.[87] Dispute policies empowered registrars to resolve disputes between registrants and trademark holders over registered domain names[88] and reflected the fact that trademark infringement was the predominant legal concern in the DNS at the time. That concern stemmed from the fact that initially, nothing stopped an individual from registering almost any available string as a domain name, even if the string consisted of a trademarked word or phrase in which the registrant possessed no rights. Coupled with the absence of registration fees before 1995, this lax registration environment gave rise to the practice of deliberately registering a company's name or trademark in hopes of selling the domain name at a high price once the less tech-savvy company belatedly realized the importance of establishing a presence in cyberspace. Famous early examples include disputes over McDonalds.com, MTV.COM, and Peta.org.[89]

This problem, colloquially termed "cybersquatting," was originally left to registrars to resolve under the terms of their registration agreements. But by 1999, after significant pressure from trademark owners, Congress enacted the Anticybersquatting Consumer Protection Act (ACPA) to provide a uniform federal framework for resolving cybersquatting disputes.[90] Under the ACPA, a person may be liable in a federal civil action by a trademark owner if that person registers, traffics in, or uses a domain name that is identical or confusingly similar to the trademark with bad faith intent to profit from the trademark.[91] If a court finds for the trademark owner in an ACPA action, the court may order the forfeiture or cancellation of the domain name or transfer the domain name to the trademark owner.[92] Moreover, to deal with the problem of cybersquatters located abroad, the ACPA provides for *in rem* jurisdiction over the disputed domain name by deeming its *situs* to be in the judicial district in which the domain

87. *See, e.g., NSI Solutions Service Agreement Version Number 2.0*, NETWORK SOLUTIONS (Dec. 2, 1998), http://web.archive.org/web/19981203102059/http://networksolutions.com/agreement_print.html [https://perma.cc/WT7X-DZMU].

88. *See, e.g., Network Solutions' Domain Name Dispute Policy*, NETWORK SOLUTIONS (Feb. 25, 1998), https://web.archive.org/web/19981202103009/http://www.networksolutions.com/dispute-rev03.html [https://perma.cc/G3SY-2QBU].

89. Matt Novak, *5 Domain Name Battles of the Early Web*, GIZMODO (Nov. 21, 2014, 1:50 PM), https://paleofuture.gizmodo.com/5-domain-name-battles-of-the-early-web-1660616980 [https://perma.cc/88XZ-B7YM].

90. *See* Consolidated Appropriations Act, 2000, Pub. L. No. 106–113, 113 Stat. 1501 (1999) (codified at 15 U.S.C. § 1125(d)(1)(A)(i)-(ii)).

91. 15 U.S.C. § 1125(d)(1)(A) (2018).

92. *Id.* at § 1125(d)(1)(C).

name registrar, registry operator, or other relevant DNS intermediary is located.[93]

Likewise, shortly after ICANN assumed the mantle of the IANA, ICANN followed suit with its own procedure for dealing with trademark disputes—the Uniform Domain Name Dispute Resolution Policy (UDRP).[94] Like the ACPA, the UDRP provides a mechanism for trademark holders to challenge the bad faith registration and use of domain names that implicate registered trademarks.[95] Unlike the ACPA, however, which requires the trademark holder to file suit in federal court, the UDRP establishes a lightweight, alternative dispute resolution framework that provides for fast and inexpensive adjudication of cybersquatting claims. Complainants may select from ICANN-accredited arbitrators, such as the World Intellectual Property Organization (WIPO), the National Arbitration Forum (NAF), or, previously, certain for-profit companies.[96] If a complainant prevails, the only available remedies are cancelation or transfer of the subject domain name.[97] However, a losing registrant may stay either remedy by challenging the decision in a court of competent jurisdiction within ten days of the ruling.[98]

Although both the ACPA and the UDRP provide a forum for IP infringement claims to be made against domain name registrants, such infringement claims are limited to trademark disputes. Moreover, a trademark claim against a domain name registrant can be stated under the ACPA or UDRP only to the extent it alleges that the domain name itself infringes the complainant's trademark.[99] Neither framework provides a cause of action against

---

93. *Id.* at § 1125(d)(2)(C); *see, e.g.*, GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 610 (E.D. Va. 2003) (permitting a trademark holder to take down an infringing domain name under the ACPA registered in South Korea, where the registrant could not be served with process and the Korean registrar had been enjoined by a Korean court from canceling the domain name).

94. *See Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy*, ICANN, https://www.icann.org/resources/pages/schedule-2012-02-25-en [https://perma.cc/VZ3X-5FBY] (last visited Oct. 18, 2020).

95. *See Uniform Domain-Name Dispute-Resolution Policy*, ICANN, https://www.icann.org/resources/pages/help/dndr/udrp-en [https://perma.cc/56KB-NYPH] (last visited Oct. 18, 2020).

96. *See List of Approved Dispute Resolution Service Providers*, ICANN, https://www.icann.org/resources/pages/providers-6d-2012-02-25-en [https://perma.cc/6N8L-X9EY] (last visited Oct. 18, 2020).

97. *Uniform Domain Name Dispute Resolution Policy*, ICANN, § 4(i) (Oct. 24, 1999), https://www.icann.org/resources/pages/policy-2012-02-25-en [https://perma.cc/NNM4-FS6Q].

98. *Id.* at § 4(k).

99. *See* Bridy, *Notice and Takedown*, *supra* note 15, at 1356 ("Trademark cases that do not involve cybersquatting cannot be adjudicated via the UDRP . . . ."); Adam

a registrant based on the *content* of any website associated with the domain. Thus, actions may not be brought under the ACPA or the UDRP against the operator of a website selling counterfeit merchandise, such as fake Gucci bags or Rolex watches, if the trademark owners' claims go to the content or operation of the website rather than the domain name used to host the website. Likewise, movie and music rights holders could not look to the ACPA or UDRP to take down a domain name associated with a website hosting pirated movies and music if the dispute concerns only copyright infringement.

Over time, registrars added restrictions to their agreements concerning how registrants may use domain names in the form of "acceptable use policies" that went beyond cybersquatting. Registrars introduced prohibitions on malicious cyber activity (spamming, phishing, and distributing malware),[100] IP piracy (copyrighted movie, music, and software sharing),[101] and other types of illegal activity (child pornography, online gambling, and money laundering).[102] While registrars might be commended for seeking to curb illegal activity, such restrictions marked a fundamental expansion of registrar authority into new territory: content regulation. In most, if not all, cases where a registrant might run afoul of an acceptable use policy, the source of the violation is content or activity occurring on a website, rather than within the domain name pointing to the website. And unless the registrant is using the registrar as a web host, such content will not be hosted or transmitted by the registrar since, as explained *supra*, no website content ever flows through the DNS.[103]

The separate nature of DNS services and website hosting have led some commentators and public interest groups to question whether registration agreements should include acceptable use policies.[104] They argue that such policies, while well-intentioned,

---

Silberlight, *Domain Name Disputes Under the ACPA in the New Millennium: When is Bad Faith Intent to Profit Really Bad Faith and Has Anything Changed with the ACPA's Inception?*, 13 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 269, 277 (2002) ("Although it is based on traditional trademark principles, the ACPA is narrowly tailored to deal with problems arising from domain name disputes.").

100. *See, e.g.*, *Registration Agreement*, ENOM, § 4(d)(ii), https://www.enom.com/terms/agreement.aspx [https://perma.cc/22NC-33WW] (last visited Oct. 18, 2020).

101. *See, e.g.*, *MyDomain's Acceptable Use Policy (AUP)*, MYDOMAIN, § 1(a)(x), https://www.mydomain.com/legal/legal-aup.html [https://perma.cc/8WYM-K428] (last visited Oct. 18, 2020).

102. *See id.* § 1(v)–(vi), (xi).

103. *See supra* Part I.A.

104. *See, e.g.*, Jeremy Malcolm & Mitch Stoltz, *Healthy Domains Initiative Isn't Healthy for the Internet*, ELECTRONIC FRONTIER FOUND. (Feb. 9, 2017), https://www.eff.org/deeplinks/2017/02/healthy-domains-initiative-censorship-through-

go beyond the legitimate scope of concern or authority of DNS intermediaries.[105] Moreover, as private actors, registrars are not well-positioned to determine the legality of registrants' behavior.[106] And to the extent they solicit help from industry players, such as the RIAA or MPAA, as "trusted notifiers" to advise on legality, such industry players may have strong incentives to take positions that benefit their financial interests.[107]

Consequences for breaching an acceptable use policy are often steep. Registrars reserve broad rights to take down domain names associated with illegal activity by suspending, canceling, or transferring the domain.[108] Suspending a domain name involves instructing the registry operator to temporarily cease resolving DNS queries for the domain name (Step 7 in Fig. 1), effectively taking down the site.[109] Canceling a registration entails instructing the registry operator to remove the registrant's information from the authoritative registry database, which would allow any other entity to register the domain name on a first-come basis.[110]

---

shadow-regulation [https://perma.cc/QY8D-4YQX] ("[A] domain name owner who contracts with a registrar is doing so *only for the domain name* of their website or Internet service. The content that happens to be posted within that website or service has nothing to do with the domain name registrar, and frankly, is none of its business."(emphasis in original)).

105. *See id.*

106. *See* Allen R. Grogan, *Community Outreach on Interpretation and Enforcement of the 2013 RAA*, ICANN (June 11, 2015), https://www.icann.org/news/blog/community-outreach-on-interpretation-and-enforcement-of-the-2013-raa [https://perma.cc/R4EV-FJEF] (noting the opinion of some registrars that they are not qualified to determine whether a registered name holder is engaged in illegal activity); *cf.* Bridy, *Notice and Takedown*, *supra* note 15, at 1375 ("trusted notifier program[s] . . . call[] on registry employees with no particular expertise or training in the law to make domain-wide determinations about the legality of content under an unspecified range of laws from an unspecified range of jurisdictions, some of which may have conflicting laws on the same subject matter.").

107. *See* Bridy, *Notice and Takedown*, *supra* note 15, at 1376 (describing a voluntary "Trusted Notifier" program established between the MPAA, RIAA, and registry operators as "loosely defined and heavily biased in favor of complainants"); Malcolm & Stoltz, *Healthy Domains Initiative Isn't Healthy for the Internet*, *supra* note 104 ("[A]ny voluntary, private dispute resolution system paid for by the complaining parties will be captured by copyright holders . . . .").

108. *See, e.g.*, *Domain Registration Agreement*, DOMAIN.COM, § 15(c), http://www1.domain.com/legal/legal-domain.html [https://perma.cc/4ZCF-FXW3] (last visited Oct. 18, 2020) ("Domain.com reserves the right to suspend, cancel, transfer or modify your domain registration if . . . you use your domain in connection with unlawful activity . . . .").

109. *See* JEFTOVIC, *supra* note 24, at 22 (describing the "clientHold" status flag that can be set by a registrar to cause a domain name not to resolve across the Internet).

110. *See* GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 620–21 (E.D. Va. 2003) ("[A] domain name is canceled by the issuance of a delete command by the domain name's current registrar," which "instruct[s] the registry to delete all information regarding the domain name from the Registry Database and the TLD zone file," at which point, "the individual domain name will once again be available for registration to any registrant on a first-come, first-served basis.").

Alternatively, a registrar may transfer the domain name directly to another registrant, as is often done in the case of a successful ACPA or UDRP action.[111]

In fact, registrars often reserve the right to terminate a registration agreement, and any domain name registrations along with it, for any breach of the agreement, no matter how minor.[112] Thus, registrars can cancel, and previously have canceled, domain name registrations for breaches as immaterial as failing to keep one's contact information up to date.[113] To be sure, market forces prevent registrars from operating with too heavy a hand in the case of otherwise harmless websites. Registrars who earn a reputation for canceling registrations of legitimate websites may soon find themselves with few remaining customers, given the ease of transferring domain names to other registrars. But other market forces may compel registrars to opportunistically seize upon any contractual basis to cancel or suspend a domain name if public pressure mounts against an unpopular group or viewpoint with which the domain name is associated.

In addition to registrars, other DNS intermediaries have seen fit to place restrictions on how registrants may use their domain names. While registry operators and ICANN typically do not have contractual privity with registrants, the contractual framework that ties together the different levels of DNS intermediaries provides a mechanism to impose flow-down terms that ultimately bind registrants.

Registrars who wish to offer domain names within a particular top-level domain name are required to execute the registry operator's "registry-registrar" agreement, which prescribes the fees charged to registrars for registering and renewing domain names on behalf of registrants and the process for using the registry operator's automated registration system.[114] In addition, many

111. *See Case Outcome (Consolidated): All Years*, WIPO, http://www.wipo.int/amc/en/domains/statistics/decision_rate.jsp [https://perma.cc/45NL-8PSC] (last visited Oct. 18, 2020) (indicating that 88% of all UDRP cases to date have resulted in a transfer of the domain name at issue).

112. *See, e.g., Domain Registration Agreement*, FASTDOMAIN, § 19, https://www.fastdomain.com/domain-registration-agreement [https://perma.cc/K9LV-JRN2] (last visited Oct. 18, 2020) (providing a right to delete a domain name registration if a registrant "fail[s] to abide by any provision of [the] Agreement").

113. *See* Andrew Allemann, *GoDaddy Deletes Domain Name for Inaccurate Email Address*, DOMAIN NAME WIRE (Feb. 27, 2007), https://domainnamewire.com/2007/02/27/godaddy-deletes-domain-name-for-inaccurate-email-address/ [https://perma.cc/J2DN-5TNE] (criticizing GoDaddy's cancelation of the domain name FamilyAlbum.COM for failing to update an invalid email address in a timely manner).

114. *See, e.g., Registry-Registrar Agreement*, IRRP.NET, §2 Exhibit F, http://www.irrp.net/NEULEVEL_BIZ_RRA.pdf [https://perma.cc/5955-LCJN] (last visited Oct. 18, 2020).

registry-registrar agreements include flow-down terms that registrars must include in their registration agreements, such as local presence requirements (in the case of certain country code top-level domains), industry membership or accreditation (in the case of certain restricted or sponsored top-level domains), and, increasingly, restrictions against illegal conduct and IP infringement.[115] Like registrars, registry operators reserve the right to cancel, suspend, or transfer the domain name of a registrant who violates such restrictions.[116]

At the IANA level, ICANN has two separate mechanisms to impose flow-down terms on registrants. For generic top-level domains, ICANN typically requires each registry operator to execute a "registry agreement," which delegates management of the top-level domain to the registry operator for a limited, ten-year period in exchange for certain reciprocal commitments.[117] ICANN also includes flow-down terms in its registry agreements that registry operators must incorporate into their registry-registrar agreements and, by extension, flow down to registrars to include in their agreements with registrants.[118] For example, ICANN's Base Registry Agreement for new generic top-level domains states:

> Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law

115. *See, e.g., Registration and Services Agreement,* PSI-USA, Exhibits C–D, https://www.psi-usa.info/psi-usa-registration_Agreement.pdf [https://perma.cc/H5HH-JHYH] (last visited Oct. 18, 2020) (presenting required flow-down terms for dozens of different top-level domains).

116. *See, e.g., Registry-Registrar Agreement v1.0,* .JOBS, Exhibit D § (d), http://goto.jobs/wp-content/uploads/2016/07/jobs_RRA.pdf [https://perma.cc/S4CZ-QBED] (last visited Oct. 18, 2020) ("Registry Operator, in its sole discretion, may revoke, cancel, deny, transfer, suspend, terminate or otherwise modify the rights of a Registered Name Holder, without any notice thereto, in the event of non-compliance by the Registered Name Holder with any provision of the Registrar's Registration Agreement, the Registry-Registrant Agreement, the registrant eligibility requirements and the use restrictions . . . .").

117. *See ICANN Mot. to Quash Writ of Attachment,* Haim v. Islamic Rep. of Iran, 784 F.Supp.2d 1, 7–9 (D.D.C. 2011) (No. 02-1811).

118. *See* A. Michael Froomkin, *Almost Free: An Analysis of ICANN's 'Affirmation of Commitments,'* 9 J. ON TELECOMM. & HIGH TECH. L. 187, 214 (2011) ("By requiring the registries—as a condition of being listed in the root—to require the registrars to include standard form terms in their contracts with registrants, ICANN gains a degree of control over registrants . . . .") [hereinafter Froomkin, *Almost Free*].

> and any related procedures) consequences for such activities including suspension of the domain name.[119]

ICANN also imposes similar policies directly on registrars through its Registrar Accreditation Agreement, which registrars must sign to become accredited to offer domain name registration services.[120] In that agreement, ICANN requires registrars to bind registrants not only to the UDRP for trademark disputes but also to representations that registrants will not use their domain names "directly or indirectly" to "infringe[] the legal rights of any third party."[121]

Figure 3 depicts the above-described multi-tier contractual framework through which registrars, registry operators, and ICANN each impose content-based restrictions on registrants.

119. *Base Registry Agreement,* ICANN, *supra* note 73, at Exhibit A, Specification 11, § 3(a).

120. *See Registrar Accreditation Agreement,* ICANN, §§ 3.7.7.9, 3.8 (2013), https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en [https://perma.cc/PG4W-UV5G].

121. *See id.*

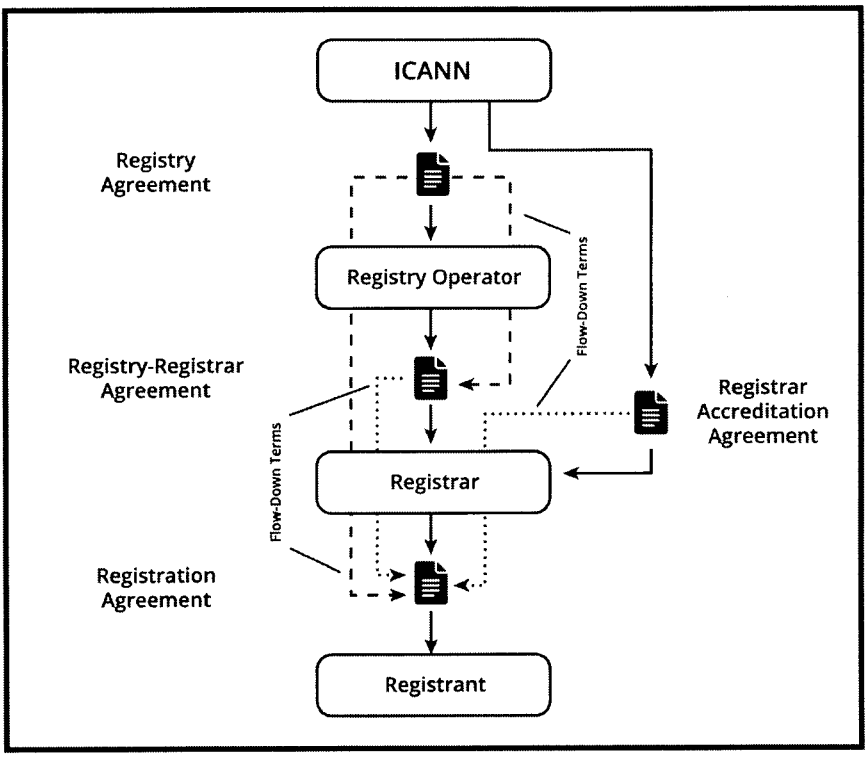


FIGURE 3

B. Restrictions against Legal Content

Whatever the merits of permitting DNS intermediaries, who play no role in hosting or delivering website content, to seize domain names associated with malware, counterfeit goods, or pirated media, their advancement into content regulation is at least understandable given the illegal nature of such activities.[122] Where DNS governance becomes harder to justify is where DNS intermediaries seek to regulate legal content or conduct based solely on moral grounds. For example, GoDaddy prohibits registrants not only from engaging in illegal activity but also from

122. Setting aside whether DNS intermediaries have or should have the legal right to seize domain names associated with illegal activity, there can be little doubt that these restrictions can protect the public from harmful practices. As a recent example, Nominet, the registry operator for the .UK country code top-level domain has taken a proactive role in identifying and suspending domain names used to host fraudulent sites selling fake vaccines, protective equipment, and fraudulent remedies related to the COVID-19 virus. *See* Daphne Leprince-Ringuet, *Domain Name Registry Suspends 600 Suspicious Coronavirus Websites*, ZDNET (Apr. 7, 2020, 4:38 PM), https://www.zdnet.com/article/domain-name-registrar-suspends-600-suspicious-coronavirus-websites/ [https://perma.cc/WA9N-ZHZ2].

"promot[ing] or encourag[ing]" illegal activity,[123] a category of content that encompasses constitutionally protected speech.[124] In addition, many registrars now include so-called "morality clauses" in their acceptable use policies that prohibit registrants from engaging in "offensive,"[125] "morally objectionable,"[126] or even "inappropriate" conduct.[127] Such conduct might include publishing "profane,"[128] "vulgar[],"[129] "embarrass[ing],"[130] "derogatory,"[131] "racist,"[132] "homophobic,"[133] or "blasphemous"[134] content. In other cases, restrictions against "morally objectionable activities" are not further defined, leaving the registrar to determine in its sole discretion whether any registrant's activities violate these amorphous standards.[135]

Some registrars abdicate even this responsibility, outsourcing it instead to the community. For example, GoDaddy reserves the right to cancel a domain name if it receives an "excessive amount of complaints" from the public about the domain name or content on

123. *Universal Terms of Service Agreement,* GODADDY, § 5(iii) (Oct. 30, 2019), https://www.godaddy.com/legal-agreements [https://perma.cc/EE4S-VBPV].

124. Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1036 n.5 (2018) ("Calls for violence or political disruption generally enjoy First Amendment protection . . . .").

125. *Terms of Service,* CRAZY DOMAINS, §2, https://www.crazydomains.com.au/privacy/terms-of-service/ (last visited Oct. 18, 2020) [https://perma.cc/4R7T-8UTV].

126. *Domain Name Registration Agreement*, WILD WEST DOMAINS, §9 (Nov. 4, 2019), https://www.secureserver.net/legal-agreement?id=reg_sa&pl_id=1387 [https://perma.cc/RC5B-KP9C].

127. *Domain Registration Agreement,* DOMAIN.COM, § 6(g)(vii), http://www1.domain.com/legal/legal-domain.html [https://perma.cc/LS2U-R7CV] (last visited Oct. 18, 2020).

128. *Terms and Conditions,* INTERNET DOMAIN SERVICE BS CORP., § 14(iv), https://internetbs.net/en/domain-name-registrations/termsandconditions.html [https://perma.cc/Z99T-M7D5] (last updated Nov. 14, 2019).

129. *E.g., Dynadot Service Agreement Version 3.5.76,* DYNADOT, § 7 (May 15, 2019), https://www.dynadot.com/registration_agreement.html [https://perma.cc/SQ9D-MNN9].

130. *Id.*

131. *E.g., Annulet Incorporated Terms and Services Agreement,* ANNULET, § 15 (June 24, 2019), https://www.annulet.com/#/content/18content/18 [https://perma.cc/7N9R-QX93].

132. *E.g., General Terms and Conditions Version 2.2014,* REALTIME REGISTER, § 5.2.3, https://www.realtimeregister.com/resources/terms-conditions/ [https://perma.cc/6DUA-TCBL] (last visited Oct. 18, 2020).

133. *Id.*

134. *E.g., General Terms and Conditions of Service,* REGISTER.IT, § 8, https://www.register.it/company/legal/condizioni-generali.html [https://perma.cc/PRC2-QPXE] (last visited Oct. 18, 2020).

135. *E.g., Domain Name Registration Services,* WEB.COM, § 3, https://assets.web.com/legal/English/DomainNameRegistrationServices.pdf [https://perma.cc/6LBL-BBDW] (last visited Oct. 18, 2020) (omitting any further definition of "morally objectionable activity").

the registrant's website.[136] Thus, even if GoDaddy itself does not object to a particular website, a vocal interest group could succeed in revoking a lawful domain name solely through a coordinated email or Twitter campaign, an alarming power to grant the public against minority opinions or controversial ideas. Still other registrars dispense with the need to find any cause for termination and reserve the unilateral right to cancel a domain name for any reason or no reason.[137]

Not limited to termination rights, registrars may also decline to register or renew any domain name.[138] Thus, if a registrar cannot point to a morality clause or other provision in its agreement that a disfavored registrant has violated, the registrar can simply refuse to renew the domain name when the current registration term ends. If the registrant fails to transfer the domain name to another registrar before that time (or is not permitted to do so[139]), the registration will automatically expire. And because automatically filtering out controversial registrants during registration may be difficult, some registration agreements allow registrars to rescind an existing registration within thirty days of

136. *Universal Terms of Service Agreement,* GODADDY, § 14(ix), https://www.godaddy.com/legal/agreements/universal-terms-of-service-agreement [https://perma.cc/2VA7-MXSL] (last updated Aug. 3, 2020).

137. *See, e.g., Registration Agreement,* NAMECHEAP, § 29, https://www.namecheap.com/legal/domains/registration-agreement/ [https://perma.cc/8Z5Y-CBZU] (last visited Nov. 26, 2019) ("Namecheap expressly reserves the right to deny, cancel, terminate, suspend, lock, or modify access to (or control of) any account or any Services (including the right to cancel or transfer any domain name registration) for any reason (as determined by Namecheap in its sole and absolute discretion) . . . .").

138. *See, e.g., Master Services Agreement,* WEB.COM, § 1(D) (Feb. 13, 2019) https://legal.web.com/?bookmarked=66DD7134F12BBFA455FDA2851270549B.janus-production [https://perma.cc/A7FW-AQ4A]; *see also, Register.com Privacy Notice,* REGISTER.COM (2001) ("Register.com may elect to accept or reject your application for registration or renewal for any reason at its sole discretion . . . .").

139. Although registrants generally have an ICANN-guaranteed right to transfer their domain names between registrars, registrars can place a domain in "Lock" status in certain circumstances to prevent transfer, such as during the pendency of a UDRP proceeding or when there is evidence of fraud. *FAQs for Registrants: Transferring Your Domain Name,* ICANN, § 8, https://www.icann.org/resources/pages/name-holder-faqs-2017-10-10-en [https://perma.cc/2WR4-XML6] (last visited Oct. 18, 2020). Registrars may also a lock a domain name for the first sixty days after the domain is registered or transferred to the registrar. *Id.* Thus, in the case of DailyStormer.COM, although GoDaddy provided the registrant with twenty-four hours to transfer the domain name to another registrar, the domain name became subject to a sixty-day lock after being transferred to Google Domains. As a result, when Google Domains then elected to terminate the registration, the domain name was within the sixty-day lock and could not be transferred to another registrar to allow the registrant to keep the domain name. *See* Andrew Allemann, *Google Took a Very Strong Stance on DailyStormer.com,* DOMAIN NAME WIRE (Aug. 15, 2017), https://domainnamewire.com/2017/08/15/google-took-strong-stance-dailystormer-com/ [https://perma.cc/T7ST-JSLA].

creation for any reason.[140] Still, registrars need not rely on non-renewal, an eventuality that may occur years later and a fate that most registrants may avoid by transferring to another registrar. Many registrars reserve the right to modify their registration agreement at any time.[141] These registrars may, therefore, introduce new acceptable use policies targeted specifically at registrants whose domain names they wish to cancel more expeditiously.

Restrictions against legal content are by no means confined to a select group of niche, activist-minded registrars. In 2017, the Internet Governance Project out of the Georgia Institute of Technology (IGP) undertook to determine the number of domain name registrations subject to morality clauses.[142] In doing so, the IGP analyzed registration agreements used by 70 different ICANN-accredited registrars, which together accounted for 90% of all gTLD domain registrations worldwide.[143] The IGP found that 59% of these registrars, which together managed more than 62% of all domain registrations, included a morality clause (or functional equivalent) in their terms of service.[144] Thus, more than half of all domain names registered on the Internet are subject to suspension, cancelation, or transfer if a registrar—or, in some cases, the community—objects to the registrant's legal activity based on subjective moral standards.

Like registrars, registry operators have sought to regulate legal content through their own morality clauses. Working through the instrumentality of flow-down provisions, some registry operators prohibit registrants from engaging in behavior that is

140. *See, e.g., Registration Agreement*, ENOM, § 6(a), https://www.enom.com/terms/agreement.aspx [https://perma.cc/5JHH-6E2A] (last visited Oct. 18, 2020) ("We . . . may reject your domain name registration application or elect to discontinue providing Services to you for any reason within thirty (30) days of a Service initiation or a Service renewal.").

141. *See e.g., Domain Management Terms and Conditions*, MARKMONITOR, § 13, https://www.markmonitor.com/legal/domain-management-terms-and-conditions [https://perma.cc/RS4F-3DBN] (last visited Oct. 18, 2020) ("MarkMonitor may modify or amend this Agreement . . . to adjust to changing business circumstances. Your continued use of any domain name registered through MarkMonitor shall constitute your acceptance of this Agreement . . . .").

142. *See generally* Brenden Kuerbis, Ishan Mehta & Milton Mueller, *In Search of Amoral Registrars: Content Regulation and Domain Name Policy*, INTERNET GOVERNANCE PROJECT (Nov. 21, 2017), https://www.internetgovernance.org/wp-content/uploads/AmoralReg-PAPER-final.pdf [https://perma.cc/BTQ5-QL3V].

143. *Id.* at 5.

144. *Id.* at 7.

"abusive,"[145] "obscene,"[146] "contrary to public order or morality,"[147] or "otherwise objectionable."[148] DotMarkets Registry Limited, a UK company that operates the .MARKETS top-level domain, prohibits registrants from engaging in "hate propaganda" or even directing "scorn" or "ridicule" at the registry operator.[149] As with registrars, registry operators may cancel, suspend, or transfer registrants' domain names if they violate such policies.[150] And some registry operators even require registrars to report any objectionable registrant activity to them.[151]

While individual registrars and registry operators remain free to construct their own terms of service, subject only to any mandatory flow-down provisions, the effort to regulate content through the DNS is becoming increasingly organized and coordinated across the industry. In 2017, the Domain Names Association (DNA), an industry group comprised of registrars and registry operators, launched a "Healthy Domains Initiative" (HDI) aimed at curbing "unhealthy" domain practices.[152] The HDI's initial policy document called for registries and registrars to implement policies and procedures to combat illegal or tortious online conduct, such as security abuse (malware, phishing, pharming), child abuse (child pornography), "rogue" online

145. *See, e.g., Acceptable Use and Takedown Policy*, QPON, https://www.dotqpon.com/wp-content/uploads/2018/06/ACCEPTABLE-USE-AND_TAKEDOWN-POLICY.pdf [https://perma.cc/599V-XSEV] (last visited Oct. 18, 2020).

146. *See, e.g., .PRO Agreement Appendix 8 Registry-Registrar Agreement, Exhibit H*, § 4, ICANN (Apr. 22, 2010) https://www.icann.org/resources/unthemed-pages/pro-appendix-8-2010-04-22-en [https://perma.cc/F6BX-EY7F].

147. *See, e.g., Registry-Registrar Agreement .FRL*, .FRL, § 6.2.5, (Mar. 2015) https://nic.frl/wp-content/uploads/2015/10/puntFRL-Registry-Registrar-Agreement-RRA-v1.4.pdf [https://perma.cc/F35N-BPQH].

148. *See, e.g., .ICU Terms and Conditions for Domain Registration*, .ICU, § 7(4)(1), https://nic.icu/terms/ [https://perma.cc/F7NP-FZ5D] (last visited Oct. 18, 2020).

149. *Acceptable Use and Anti-Abuse Policy*, DOTMARKETS.COM, https://nic.markets/media/1154/acceptable-use-and-anti-abuse-policy_markets.pdf [https://perma.cc/2X55-YZMF] (last updated June 2015).

150. *See, e.g., .ME Registry-Registrar Agreement*, .ME, § 2.7.2, https://domain.me/wp-content/uploads/2014/10/RegistryRegistrarAgreement.pdf [https://perma.cc/S9VH-27T5] (last visited Oct. 18, 2020) ("Registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status . . . for violations of this Agreement . . . .").

151. *See, e.g., Acceptable Use and Takedown Policy*, *supra* note 145 ("Registrars must also notify the Registry Operator's technical services provider of any abuse or malicious conduct (as defined above) of which the Registrar has knowledge, if relevant.").

152. *Domain Name Association Unveils Healthy Domains Initiative Practices*, DOMAIN NAME ASS'N (Feb. 8, 2017), https://thedna.org/domain-name-association-unveils-healthy-domains-initiative-practices/ [https://perma.cc/89PE-VDWH].

pharmacies, and copyright infringement.[153] The HDI recommended that DNS intermediaries work to combat these activities by incorporating sample clauses in their acceptable use policies, implementing trusted notifier programs, and suspending or deleting affected domain names.[154]

The HDI is both an attempt to influence industry practice and a reflection of an already advancing trend toward greater content regulation by DNS intermediaries. According to the HDI, 78% of DNA members already employ contractual provisions and procedures similar to those recommended by the HDI, and 89% of DNA members plan to *expand* the list of online practices they intend to regulate.[155]

While ICANN has so far resisted pressure to directly police legal content through its exercise of the IANA function,[156] it has nonetheless encouraged efforts by other DNS intermediaries to do so[157] and has even instituted policies and procedures that may contractually require registrars and registry operators to censor. Under ICANN's New gTLDs Program, which governs how registry operators may apply to create and manage new top-level domains, third parties can object to any applied-for string, or the manner in which the applicant intends to operate the new top-level domain, as "contrary to general principles of international law for morality and

153. *Id.* However, after significant pressure from the Electronic Frontier Foundation, the DNA withdrew its proposal for a "new compulsory arbitration system to confiscate domain names of websites accused of copyright infringement." Jeremy Malcom, *Healthy Domains Revisited: the Pharmaceutical Industry*, ELECTRONIC FRONTIER FOUND. (Mar. 2, 2017), https://www.eff.org/deeplinks/2017/03/healthy-domains-revisited-pharmaceutical-industry [https://perma.cc/VH6G-YY3K].

154. *See generally* DNA Healthy Domains Initiative, *Registry / Registrar Healthy Practices*, DOMAIN NAME ASS'N (Feb. 2017), http://thedna.org/wp-content/uploads/2017/02/DNA_Healthy_Practices_2017.pdf [https://perma.cc/T2E7-A87Y].

155. *Id.* at 2.

156. *See* Allen R. Grogan, *ICANN Is Not the Internet Content Police*, ICANN (June 12, 2015), https://www.icann.org/news/blog/icann-is-not-the-internet-content-police [https://perma.cc/Y23S-LMP2] (resisting pressure from various stakeholders to help police blasphemy, hate speech, pornography, and other categories of content that may be illegal in certain countries).

157. *See Letter from Stephen D. Crocker, Chair of the Bd., ICANN, to Greg Shatan, President, Intellectual Prop. Constituency* 1–4 (June 30, 2016), https://www.icann.org/en/system/files/correspondence/crocker-to-shatan-30jun16 [https://perma.cc/EYR8-JED3] (expressing ICANN's support of the Healthy Domains Initiative); Allen R. Grogan, *Meeting Transcript, MARRAKECH—Industry Best Practices*, ICANN (Mar. 9, 2016), https://meetings.icann.org/en/marrakech55/schedule/wed-dna-healthy-domains-initiative/transcript-dna-healthy-domains-initiative-09mar16-en [https://perma.cc/7EY7-HEGN] (quoting ICANN's Chief Contract Compliance Officer in characterizing the Healthy Domains Initiative as "the kind of voluntary initiatives that I think can be constructive.").

public order," or "detriment[al] to a broadly defined community."[158] Objections are reviewed by a panel of independent experts, which may approve or deny the application based on whether the applicant has demonstrated that it will police content under the top-level domain, either by restricting registration or by prohibiting certain forms of content.[159] If the applicant is ultimately awarded the new string but fails to substantially enforce any "Public Interest Commitments" it made in its application—which may include commitments to enforce content-based restrictions—third parties can again challenge the delegation and cause ICANN to revoke the registry operator's management of the top-level domain.[160] Thus, an expectation of content regulation and mechanisms to enforce it have effectively been built into the structure of the New gTLDs Program, and it may not be long before such policies and procedures are extended to legacy top-level domains, such as the all-important .COM.[161]

In the same manner, ICANN has foisted potential content regulation responsibilities onto registrars through its new Registrar Accreditation Agreement, which requires registrars to "take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse."[162] Unfortunately, the RAA neither defines "abuse" nor prescribes the "reasonable and prompt steps" that registrars must take.[163] But simply by forcing registrars to maintain such contacts, ICANN increases the likelihood that registrars will feel compelled to take action against a domain name if members of the public contact the registrar to allege that a given website is "abusive."[164] In that event, a registrar could very well conclude that ICANN's term is capacious enough to include the same kinds of objectionable, but legal, behavior catalogued in registrar or registry operator morality clauses.

158. *See* Bricteux, *ICANN's New gTLDs*, *supra* note 84, at 233–35.

159. *Id.* at 235–40.

160. *See Registry Agreement, Specification 11,* ICANN, § 2, (July 31, 2017), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf [https://perma.cc/339U-CZGL].

161. *See* Bricteux, *ICANN's New gTLDs*, *supra* note 84, at 244–45.

162. *Registrar Accreditation Agreement*, ICANN, § 3.18, (June 27, 2013), https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf; [https://perma.cc/PG4W-UV5G]. *See* JEFTOVIC, *supra* note 24, at 15 (showing a "Registrar Abuse Contact" as part of a domain name record).

163. *See* Bridy, *Notice and Takedown*, *supra* note 15, at 1370–72 (chronicling the debate between right holders and DNS intermediaries as to registrars' enforcement obligations under the anti-abuse provision).

164. *See* Bricteux, *ICANN's New gTLDs*, *supra* note 84, at 244.

C. *Examining DNS Censorship*

Commentators have criticized the practice of taking down domain names based on legal website content as a form of "private censorship."[165] Clearly, by itself, private censorship does not implicate constitutional concerns, since the Supreme Court has long held that the First Amendment applies only to actions by the state.[166] While the public function doctrine operates as a limited, narrow exception to the state action requirement, that doctrine has never been applied to cyberspace, and at least one recent case suggests that the Supreme Court is not likely to do so.[167]

Moreover, as scholars have noted, in some cases, private censorship may represent simply the exercise of traditional intermediary functions, such as protecting users from dangerous content or providing curated experiences to match consumer interests, both of which may be beneficial.[168] And the exercise of editorial discretion—also technically a form of private censorship—can itself further important free speech interests.[169] It therefore warrants examining whether DNS censorship furthers the same benefits as other forms of private censorship, such as might be exercised by search engines and social media networks, or whether DNS censorship is different in nature. In the subsections that follow, I present three arguments for why DNS censorship presents unique threats to free expression on the Internet.

1. "Dumb Pipes"

One concern with DNS censorship is that it seeks to regulate content that is wholly external to the DNS. To borrow from another debate within Internet governance, proponents of "network neutrality" argue that the Internet was designed as a "dumb" network in which its foundational protocols (the TCP and IP

165. *See, e.g.*, Dorf, *supra* note 14; Corynne McSherry et al., *Private Censorship Is Not the Best Way to Fight Hate or Defend Democracy: Here Are Some Better Ideas*, ELECTRONIC FRONTIER FOUND. (Jan. 30, 2018), https://www.eff.org/deeplinks/2018/01/private-censorship-not-best-way-fight-hate-or-defend-democracy-here-are-some [https://perma.cc/JCP4-8B7X]; Jerry Malcom et al., *Fighting Neo-Nazis*, *supra* note 13.

166. Yoo, *supra* note 16, at 699 ("Under current law, the First Amendment only restricts the actions of state actors and does not restrict the actions of private actors").

167. *See* Alison Frankel, *A Supreme Court Case Has Internet Companies Running Scared*, REUTERS (Dec. 13, 2018, 2:46 PM), https://www.reuters.com/article/us-otc-halleck-firstamendment/a-supreme-court-case-has-internet-companies-running-scared-idUSKBN1OC2XR [https://perma.cc/V6Z4-ST8F] (opining that the Supreme Court's decision against characterizing public-access television as a state actor in Manhattan Community Access Corp. v. Halleck, 139 S. Ct. 1921 (2019), indicates that the Supreme Court is unlikely to apply the public function doctrine to private Internet companies).

168. *See* Yoo, *supra* note 16, at 703–09.

169. *Id.* at 726–29.

protocols) functioned only to transmit packets of data without asking questions about the sender of the packet, the recipient, or its content.[170] This "end-to-end" principle, proponents argue, was instrumental to the growth and success of the Internet and remains foundational to the principle of a fair and open Internet.[171] Internet service providers should therefore provide only dumb pipes and should not be permitted to advantage some content over other content in terms of access, transmission speed, or prioritization.[172]

Without wading into the merits of network neutrality itself, I note that to the extent the "dumb pipes" argument counsels in favor of prohibiting content discrimination by Internet Service Providers (ISPs), it provides an even more compelling argument against DNS censorship. Like ISPs, DNS intermediaries provide core network services that make Internet communications possible. From an openness and fairness perspective, we should expect DNS intermediaries to register, renew, and resolve domain names without regard to the identity of the person who hosts an associated website or the content on that website. But unlike ISPs, DNS intermediaries provide no pipes, whether smart or dumb, for website content. As noted *supra*, no website content ever flows through the DNS or through registrars, registry operators, or ICANN in their role as DNS intermediaries.[173] The sole function of DNS infrastructure is to provide a name-to-address mapping system that can be used to locate content.[174] Once located, that content flows through other parties' pipes.[175] It therefore makes even less sense to allow DNS intermediaries to disadvantage website owners based on content that does not even flow through DNS pipes.[176]

If the DNS truly is the "phonebook of the Internet,"[177] then canceling a domain name is not unlike removing a company's name and address from a traditional phonebook. While we might support

170. Paul Ganley & Ben Allgrove, *Net Neutrality: A User's Guide*, 22 COMPUTER L. & SECURITY REP. 454, 456 (2006); Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 146–47 (2003).

171. Ganley & Allgrove, *supra* note 170, at 456.

172. *See* Wu, *supra* note 170, at 165–70.

173. *See supra*, Part I.A.

174. *Cf.* Bridy, *Notice and Takedown*, *supra* note 15, at 1382 (characterizing online copyright infringement as "external to the navigational operation of the DNS").

175. Typically, pipes provided by Internet service providers. *See supra*, Part I.A.

176. *See* Malcom et al., *Fighting Neo-Nazis*, *supra* note 13 ("Domain name registrars have even less connection to speech than a conduit provider such as an ISP, as the contents of a website or service never touch the registrar's systems.").

177. *See* SOENKE ZEHLE, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, THE WILEY–BLACKWELL ENCYCLOPEDIA OF GLOBALIZATION 1191 (Blackwell Publishing Ltd., 2012); *see* Klint Finley, *The Internet Finally Belongs to Everyone*, WIRED (Oct. 3, 2016, 12:09 PM), https://www.wired.com/2016/10/internet-finally-belongs-everyone/ [https://perma.cc/6CQC-36LD].

the de-listing of proven criminal enterprises, we would object to removing the contact information of a law-abiding entity, such as a strip club or unpopular political organization, simply because some might find that entity's activities or viewpoints to be morally objectionable. The latter should not be within the purview of a phonebook company that holds itself out to the public as an authoritative, comprehensive, and reliable omnibus of all registered entities within a geographical area. Likewise, the DNS has historically held itself out as, and the Internet community has viewed it as, an authoritative, comprehensive, and reliable omnibus of all hosts on the Internet that are intended to be publicly accessible.[178] The DNS should no more attempt to regulate website content by making websites unreachable than a phonebook company should attempt to improve public morality by making strip clubs difficult to locate.

2. Censorship Creep and Collateral Censorship

To be sure, some might be inclined to support DNS censorship depending on the nature of the websites so targeted. After all, the three registrants referenced in the Introduction all faced suspension or cancellation of their domain names due to bigoted or hateful speech found on their websites. If the primary effect of DNS censorship is to make it harder to locate "vulgar," "derogatory," or "blasphemous" websites, then far from being problematic, proponents might argue, DNS censorship may represent an important tool in the fight for a healthy and tolerant Internet. Viewed from this perspective, DNS intermediaries may even have a moral duty to practice DNS censorship as a matter of corporate social responsibility.

Some groups certainly take this position. A group of civil rights, human rights, technology policy, and consumer protection organizations called the "Change the Terms" coalition has created recommended corporate policies and terms of service with the goal of helping technology companies combat hate online.[179] One of the coalition's model terms states, "[u]sers may not use [the provider's] services to engage in hateful activities or use [the] services to facilitate hateful activities engaged in elsewhere, whether online or

178. *See, e.g.*, ICANN Bylaws, Art. I, § 2.3 ("ICANN shall not apply its standards, policies, procedures, or practices inequitably or single out any particular party for disparate treatment unless justified by substantial and reasonable cause, such as the promotion of effective competition."); Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy*, 18 INFO. SOC'Y 193, 195 (2002) ("At the heart of the DNS is the Internet's *name space*. The name space lists (nearly) all computers on the Internet.").

179. *See* CHANGE THE TERMS, https://www.changetheterms.org [https://perma.cc/LN79-HYXA] (last visited Oct. 18, 2020).

offline."[180] Because online service providers who include such restrictions would presumably have the right to terminate services for a breaching customer, and because "domain name service providers" are intended adopters of these terms, the coalition is effectively calling for DNS intermediaries to use the threat of domain name cancelation to police online (and even offline) content.[181]

But if history teaches anything, censorship that is initially limited to one category of content rarely remains so confined. The phenomenon of "censorship creep," by which is meant "the expansion of speech policies beyond their original goals,"[182] is well documented in the literature. As one commentator noted, "when you build a censorship system for one purpose, you can be pretty certain that it will be used for other purposes."[183] Nor is private censorship, including speech restrictions imposed by U.S. technology companies, immune from this phenomenon. As Danielle Keats Citron chronicled, U.S. technology companies, including Twitter and Google's YouTube, initially resisted pressure to remove terrorist propaganda from their platforms, adhering instead to free speech policies that were largely consistent with First Amendment doctrine.[184] After U.S. technology companies changed course and agreed to voluntarily cooperate with European regulators in 2016 to remove terrorist propaganda, it was not long before the scope of prohibited material expanded to other categories, such as "fake news" and generalized "hate speech."[185] The problems of definitional ambiguity and imperfect automation have even led to the banning of users engaged in political dissent or legitimate

180. *Adopt the Terms*, CHANGE THE TERMS, https://www.changetheterms.org/terms [https://perma.cc/7BV5-AW3L] (last visited Oct. 18, 2020). Notably, the coalition extends prohibition further than many DNS intermediaries by encouraging online service providers to examine even *offline* conduct.

181. *Id.* Curiously, the coalition expressly notes that due to its commitment to "an open internet," its policies "are not intended to be used by Internet Service Providers"—a clear nod to network neutrality. *See FAQs*, CHANGE THE TERMS, https://www.changetheterms.org/faqs [https://perma.cc/WVF8-YRZ3] (last visited Oct. 18, 2020). The distinction between social media, video sharing, and web hosting companies, which are encouraged to adopt the coalition's terms, and ISPs, which are not, certainly makes sense. This distinction no doubt lies in the fact that the former can be expected to exercise editorial discretion, whereas the latter, which provide foundational Internet services, should not, out of a commitment to "an open internet." But, as should be clear from the above discussion, the services DNS intermediaries provide are just as foundational to the operation of the Internet. It therefore makes far more sense to lump DNS intermediaries in with ISPs than with social media platforms.

182. Citron, *supra* note 124, at 1051.

183. Paul Bernal, *Censorship and Surveillance . . .*, PAUL BERNAL'S BLOG (Sept. 25, 2014), https://paulbernal.wordpress.com/2014/09/25/censorship-and-surveillance/ [https://perma.cc/LP6L-3N28] (as quoted in Citron, *supra* note 124, at 1051).

184. Citron, *supra* note 124, at 1036–37.

185. *See id.* at 1052.

debate on hot-button issues such as minority users who repost racist messages directed at them on online platforms.[186] As Citron notes, well-intentioned censorship may inadvertently work against its own goals by suppressing "legitimate debate and counter speech that might convince people to reject bigotry and terrorist ideology."[187]

DNS censorship is no less likely to experience scope creep and produce unintended consequences with the passage of time. The joint problems of definitional ambiguity, imperfect automation, and public pressure could very well combine to eventually expand DNS censorship to other unpopular viewpoints, or to chill legitimate dissent or debate. In this, proponents of DNS censorship might consider that one of the main techniques used by authoritarian regimes to block dissident or disfavored online content is to block websites through the DNS.[188] And thus, proposals to encrypt DNS queries are gaining in popularity, with the goal of helping persons under authoritarian regimes circumvent Internet censorship.[189]

Even the U.S. government, which is bound by the First Amendment, has engaged in a form of "collateral censorship"[190] by pressuring DNS intermediaries to take action against domain names associated with suspected illegal activities as an end-run around official judicial processes. In 2012, the Secret Service secured GoDaddy's agreement to suspend JOTFORM.COM after one of JotForm, Inc.'s customers was suspected of using the service

---

186. *Id.* at 1050 n.97.

187. *Id.* at 1050.

188. Oliver Farnan et al., *Poisoning the Well—Exploring the Great Firewall's Poisoned DNS Responses,* ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOC'Y, § 1 (2016) ("One of the key technical methods used by the [Great Firewall] is DNS poisoning."); *see Perspectives on Internet Content Blocking: An Overview*, INTERNET SOC'Y (Mar. 24, 2017) https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/ [https://perma.cc/68U4-5VL5]; MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 197 (2010) ("More governments and censorship advocates have begun to think that blocking or 'filtering' techniques [within the DNS] could recreate the kind of control they once had over traditional territorial media.").

189. *See EFF and Partners Urge U.S. Lawmakers to Support New DoH Protocol for a More Secure Internet*, ELECTRONIC FRONTIER FOUND. (Oct. 22, 2019), https://www.eff.org/press/releases/eff-and-partners-urge-us-lawmakers-support-new-doh-protocol-more-secure-internet [https://perma.cc/ZK2M-EGQN] ("Countries like China and Turkey have used control over DNS to block their citizens' access to websites and track the web activity of activists, a form of censorship that will eventually be much more difficult once there is widespread implementation of [DNS over HTTPS].").

190. *See* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298 (2014) (providing examples of "collateral censorship, in which the state regulates party A in order to control speaker B"). New-school techniques of speech regulation operate by "[r]egulat[ing] speech through control over digital networks and auxiliary services like search engines, payment systems, and advertisers; instead of focusing directly on publishers and speakers, they are aimed at the owners of digital infrastructure." *Id.*

to facilitate a phishing scheme, an extreme move that took down the online business and left 700,000 other customers without service.[191] In 2014, the FDA successfully pressured easyDNS, a Canadian registrar, to take down a domain name associated with an allegedly illegal online pharmacy, despite the FDA's lack of jurisdiction over easyDNS or the online pharmacy.[192]

These practices stand to reason. A government that lacks jurisdiction over a website hosted abroad will see DNS resolution blocking as the most efficient way to prevent its citizens from accessing the website.[193] And if the domain name was registered with a registrar or registry operator having a local presence, compelling or simply pressuring the DNS intermediary to suspend or cancel the domain name may succeed in taking the target website offline globally. That a single government or DNS intermediary may easily remove global access to a website simply by targeting the website operator's domain name certainly resonates with Sir Tim Berners-Lee's description of DNS as the "Achilles heel of the Web."[194]

3. Disproportionate Effects

Finally, depending on the actions taken by the DNS intermediary and the role of the intermediary in the DNS hierarchy, DNS censorship can have severe consequences for

---

191. *See* Nate Anderson, *Takedowns Run Amok? The Strange Secret Service/GoDaddy Assault on JotForm*, ARS TECHNICA (Feb. 16, 2012, 3:44 PM), https://arstechnica.com/tech-policy/2012/02/secret-service-asks-for-shutdown-of-legit-website-over-user-content-godaddy-complies/ [https://perma.cc/HSL8-U4JW].

192. *See* Mark E. Jeftovic, *Here's Why We Took Down A Pharmacy Domain Without A Court Order*, EASYDNS TECHNOLOGIES (Aug. 15, 2014), https://easydns.com/blog/2014/08/15/heres-why-we-took-down-a-pharmacy-domain-without-a-court-order/ [https://perma.cc/MR36-U8KT] (describing the Easy DNS's acquiescence to the FDA's repeated entreaties to "do the right thing"); *see also* Catalin Cimpanu, *New York Asks Domain Registrars to Crack Down on Sites Used for Coronavirus Scams*, ZDNET, https://www.zdnet.com/article/new-york-asks-domain-registrars-to-crack-down-on-sites-used-for-coronavirus-scams/ [https://perma.cc/QQV7-8MS9] (Mar. 23, 2020, 23:41 GMT) (describing efforts by New York's Attorney General to pressure six of the Internet's largest registrars "to deploy countermeasures that would make the registration of all COVID-19 and coronavirus-related domains much harder").

193. *See* Annemarie Bridy, *Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy*, 684 ARIZ. ST. L. J. 683, 709–12 (2014) [hereinafter Bridy, *Carpe Omnia*] (detailing various federal initiatives in which thousands of domain names have been seized on suspicion of illegal infringement); *see also id.* at 691 n.44 ("Many of the registrants whose domain names are being seized in [such raids] are foreign nationals over whom U.S. courts have no *in personam* jurisdiction.").

194. *Isn't it semantic?*, BCS (Sept. 3, 2006), https://www.bcs.org/content-hub/isnt-it-semantic/ [https://perma.cc/Q977-8TQM]; *accord* Malcolm & Stoltz, *Threats*, *supra* note 15 ("The domain names we use to connect to websites and Internet services are one of the weak links for free speech online: a potential point of control for governments and businesses to regulate others' online speech and activity.").

website operators, including the loss of valuable assets, business disruption, appropriation of goodwill and traffic, and potentially the systematic purging of certain minority viewpoints from the Internet.

As to the first consequence, a domain name may be extremely valuable[195] depending on the nature of the second-level string, the top-level domain, and how much goodwill has been accumulated in the domain name. The value of the second-level string will depend, in part, on lexical features, such as length and the absence of numbers or dashes; semantic distinction, such as inclusion of meaningful words; and mnemonic value, such as memorability or guessability.[196] A registrant who managed to obtain a domain name that rates highly along these dimensions may have little hope of finding a comparably valuable replacement if her original domain is seized.

While the registrant could potentially find the same, or a comparable, second-level string in another top-level domain, it is well established that different top-level domains carry different economic and reputational value.[197] Just as SEX-18273.COM is no substitute for SEX.COM, the registrant deprived of HERITAGE.ORG could take little comfort in the availability of HERITAGE.NINJA. Even if a substitute string of comparable lexical value is available in the same top-level domain, the primary value of a lost domain name may instead lie in the goodwill accrued in the name. By itself, "google," an intentional misspelling of the word "googol," may carry only marginal intrinsic value. Still, GOOGLE.COM retains the title of most visited website[198]—and, therefore, likely also the most valuable domain name in the world—almost entirely on account of the goodwill accrued in the string through popular usage.

---

195. *See* Joe Styler, *The Top 25 Most Expensive Domain Names*, GODADDY (June 18, 2019) https://www.godaddy.com/garage/the-top-20-most-expensive-domain-names/ [https://perma.cc/D6CG-HJJG] (listing the twenty-five most expensive domain name sales publicly reported, each domain name being sold for more than five million dollars).

196. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 62, Box 2.1 (listing various factors that contribute to the economic worth of a given domain name); MIRAMIRKHANI ET AL., *supra* note 67, at 3–4 (offering additional factors).

197. Dan Virgillito, *Which Domain Extensions Rank The Best in Google?*, SEOBLOG (Mar. 22, 2017) https://www.seoblog.com/domain-extensions-rank-google/ [https://perma.cc/8F42-Z9GW] (comparing the relative value of different top-level domains in terms of search engine optimization); Benjamin Edelman, *Priced and Unpriced Online Markets*, 23 J. ECON. PERSP. 21, 30 (2009) (noting that competing .BIZ, .INFO, and .US top-level domains carry less cachet than .COM).

198. *See* Martin Armstrong, *The World's Most Popular Websites*, STATISTIA, https://www.statista.com/chart/17613/most-popular-websites/ [https://perma.cc/SV44-ZNLX] (last visited Oct 18, 2020) (showing GOOGLE.COM with 79.62 billion visits in October 2019 and YOUTUBE.COM, the second-ranked domain, with 28.85 billion visits).

For companies with a significant online presence, losing a domain name can significantly disrupt business. For companies that operate primarily or exclusively online—so-called "born in the cloud" companies—domain name seizure represents an existential threat. Losing a domain name effectively causes a registrant's website to go offline. Even if an online business manages to establish a replacement domain name—a proposition that may take days or weeks depending on the complexity of the website—the intervening downtime will inflict injuries from which some websites may never recover. If the website provides services to business customers, downtime could subject the owner to claims for breach of contract, or customers may elect to take their business elsewhere in response to the perceived unreliability of the service.[199]

Even if a website owner manages to immediately failover to an alternate domain name, there may be downstream dependencies on the original name. If the website receives significant traffic from links on third-party websites pointing to the original domain name, that traffic will be lost, and it may take years to replace it through the organic growth of links pointing to the new name.[200] Such links further play a role in a website's search engine rankings, which may be damaged or lost as well.[201] Moreover, no matter how quickly a website is migrated to a replacement domain name, if the website owner lacks the means to contact users directly, users may have no way of even learning about the new domain name, since the website owner will not be able to publish any kind of notice reachable through the original domain known to users. Instead, users who attempt to navigate to the original domain name will either see an error message, and potentially conclude that the website has shut down, or a website belonging to a new owner, and potentially take their business to the new owner going forward.[202]

The last consequence of DNS censorship—the systematic purging of certain minority viewpoints from the Internet—has been limited thus far.[203] However, it threatens to become a greater

199. *See, e.g.*, Anderson, *supra* note 191 (quoting feedback from customers who vowed to cancel their subscriptions after JotForm Inc. was forced to migrate from JOTFORM.COM to JOTFORM.NET).

200. *See generally* MIRAMIRKHANI ET AL., *supra* note 67.

201. *See* David Trounce, *20 Reasons Why Your Search Engine Ranking & Traffic Might Drop*, SEARCH ENGINE J. (Aug. 23, 2018), https://www.searchenginejournal.com/why-search-rankings-traffic-drop/264617/ [https://perma.cc/T4XY-QBJG].

202. *See* MIRAMIRKHANI ET AL., *supra* note 67, at 257 ("When the associated domain name expires, the new registrant inherits the residual trust of the domain name and can take over its previous clients, visitors, and dependent resources").

203. *But see* Carl Schreck, *Russian Web Host Suspends Daily Stormer After Government Inquiry*, RADIO FREE EUROPE/RADIO LIBERTY (Aug. 16, 2017),

problem the more aggressively DNS intermediaries seek to regulate content based on vague notions of morality and the higher the level of enforcement from within the DNS hierarchy.[204]

Threatened with DNS censorship by a registrar, a registrant's ability to protect her domain name depends only on her ability to transfer the name before the current registrar takes action and her ability to find a new registrar with more lenient acceptable-use policies. With over two thousand ICANN-accredited registrars in the market,[205] including some who market themselves as free speech-friendly,[206] our registrant should have little trouble with the latter. As a last resort, a marginalized registrant could even complete the process of becoming accredited as her own registrar, thus defusing the threat of DNS censorship by third-party registrars altogether.[207]

If, however, a registrant faces DNS censorship courtesy of a registry operator, her options dwindle. Because each top-level domain is managed by a single registry operator, a registrant cannot evade registry-imposed content policies by switching to a different registry operator unless she is also willing to move to a different top-level domain. But changing the top-level domain associated with a domain name is equivalent to losing the original domain name altogether and replacing it with a new domain name, one that may be considerably less valuable or even unavailable. The result is that a registrant who faces suspension, cancellation, or transfer by her registry operator has no option to preserve her domain absent legal recourse. Thus, while the owners of DAILYSTORMER.COM and GAB.COM managed to keep their domain names by transferring to new registrars, the owner of

---

https://www.rferl.org/a/u-s-neo-nazi-website-russian-domain-daily-stormer/28680409.html [https://perma.cc/9SAV-4Y86] (recounting Daily Stormer founder, Andrew Anglin's, assessment that after having lost four domain names and running up against registry operators' prohibitions, he was effectively banned from registering a domain name and kicked off the Internet).

204. *See* Editorial Board, *If the Internet Belongs to Everyone, that Includes Gab*, WASH. POST (Nov. 4, 2018) ("Gab's plight highlights a central conundrum of digital governance. It is one thing for a site to tell a user they must take their hate elsewhere. It is another for the actors who control the Internet's infrastructure to prevent the site itself from operating").

205. *See Descriptions and Contact Information for ICANN-Accredited Registrars*, ICANN, https://www.icann.org/registrar-reports/accreditation-qualified-list.html [https://perma.cc/U75K-JPKH] (last visited Oct 18, 2020).

206. *See, e.g.*, Rob Monster, *Why Epik Welcomed Gab.com*, EPIK (Nov. 3, 2018), https://epik.com/blog/why-epik-welcomed-gab-com.html [https://perma.cc/X9LP-9FTA] (explaining registrar Epik's decision to sponsor GAB.COM on free-speech principles after the domain was dropped by GoDaddy).

207. *See How to Become a Registrar*, ICANN, https://www.icann.org/resources/pages/accreditation-2012-02-25-en [https://perma.cc/V9EG-DXZ4] (last visited Oct. 18, 2020).

INCELS.ME was powerless to maintain the domain name after the .ME registry operator decided to suspend it.

Likewise, if ICANN eventually reaches a point where it begins imposing robust, top-down morality restrictions, a censored registrant will not be able to save her domain name, even by attempting to migrate to a different top-level domain. Because ICANN sits atop the DNS governance hierarchy, no other domain name could be registered as a substitute for the website if the offending content remains in place. That content would effectively be banned from the Web. Without question, the content could remain accessible through the Internet outside of the DNS. The website could be accessed, and linked to, using its IP address, or the content could be distributed via other application-layer means, such as peer-to-peer applications, email, or FTP. But these alternatives would be poor substitutes for a conventional, DNS-accessible website, the predominant medium through which news and ideas are made globally accessible. Moreover, the notion that a single, private entity could set content policy for the entire DNS-accessible Web, a policy that might restrict constitutionally protected speech by all Internet users in the U.S., is an alarming possibility and one that deserves careful attention now that ICANN is no longer subject to U.S. oversight.

III. PROPERTY RIGHTS IN DOMAIN NAMES

Given this background, one wonders if a registrant has any option to protect herself from DNS censorship if a DNS intermediary is determined to stamp out her viewpoint. After all, since DNS intermediaries reserve broad rights to suspend, cancel, or transfer domain names in their contracts, a registrant can protect herself from DNS censorship only by demonstrating a superior right to the disposition of her domain name. In this article, I argue that registrants' property interests provide that superior right. However, to make that case, it is first necessary to analyze whether domain names qualify as property and, if so, what interests registrants acquire in that property. In this Part, I show that domain names are best characterized as intangible, personal property, as most courts that have considered the issue have held. To do so, I trace the history of the case law, as courts first appeared to reject and then later clearly embraced the property status of domain names. I then summarize the best arguments for such a classification and answer some of the lingering objections that courts have failed to address adequately. Next, having established the property nature of domain names, I turn to a question that, curiously, has received no attention in the literature to date: which party has title to that property? Using property theory as a guide

and weighing competing claims to ownership that might be made by other parties, I conclude that title to a registered domain name lies with its registrant and not with any DNS intermediary.

A. Domain Names as Contractual Rights

The best argument against characterizing domain names as property is that domain names do not, and cannot, exist outside of the services provided by DNS intermediaries. Standing on this rationale, the earliest cases to consider the issue suggested, but did not squarely hold, that domain names are mere contractual rights and not property. For example, in the 1999 case of *Dorer v. Arel*, faced with the issue of whether a judgment creditor could levy a domain name registered to a judgment debtor to satisfy a judgment, the U.S. District Court for the Eastern District of Virginia held that it could not.[208] The court noted that under Virginia law, a writ of *fieri facias* could be used only to levy a debtor's "personal property."[209] But a domain name registration, the court found, represented only the "product of a contract for services" between the registrar and the registrant.[210]

Likewise, in *Network Solutions, Inc. v. Umbro Int'l, Inc.*, the Virginia Supreme Court denied a plaintiff's request to garnish various domain names registered to a defendant to satisfy a default judgment.[211] Citing *Dorer*, the court held that "[a] contract for services is not 'a liability' as that term is used in [the Virginia garnishment statute] and hence is not subject to garnishment."[212] As additional support, the court noted that a registrant's right to use a domain name is "inextricably bound to the domain name services" that a registrar provides, and that "[w]hatever contractual rights the [registrant] has in the domain names . . ., those rights do not exist separate and apart from [the registrar's] services that make domain names operational Internet addresses."[213] The court also feared that allowing domain names to be garnished would allow any contractual right under a service contract—for example, prepaid satellite television services—to be garnishable.[214]

Although *Dorer* and *Umbro* have both been cited for the proposition that domain names are contractual rights rather than property, their holdings are not so clear. In *Dorer*, after suggesting that a domain name represented only the "product of a contract for

208. 60 F.Supp.2d 558, 559–61 (E.D. Va. 1999).
209. *Id.* at 559.
210. *Id.* at 561.
211. Network Solutions v. Umbro, 529 S.E.2d 80, 86 (Va. 2000).
212. *Id.*
213. *Id.*
214. *Id.* at 86–87.

services," the court ultimately declined to rule on the property status of domain names, finding instead that the plaintiff already had an adequate remedy under trademark law through the registrar's dispute resolution procedure.[215] Similarly, during oral argument in *Umbro*, the registrar had already conceded that the right to use a domain name is a form of intangible personal property.[216] And the court found that it was not essential to outcome of the case to determine whether domain names are a form of intellectual property but instead limited its holding to the fact that domain names were not "liabilities" under the Virginia garnishment statute.[217] Thus, while the *Dorer* and *Umbro* courts suggested that domain names are contractual rights rather than property, neither court explicitly held so.

B. Domain Names as Property

It wasn't until the 2003 case of *Kremen v. Cohen* that a court squarely addressed the property status of domain names.[218] In *Kremen*, the owner of SEX.COM sued Network Solutions after the registrar was defrauded into transferring the domain name to another party.[219] Because the domain had originally been registered in 1994, when Network Solutions was under contract with the National Science Foundation to provide domain names for free, no contract governed the plaintiff's registration.[220] Without a basis to assert a claim for breach of contract, the plaintiff argued that in transferring the domain name to another party without his consent, Network Solutions had tortiously converted his personal property.[221]

In evaluating this novel argument, the Ninth Circuit first applied a three-part test to determine whether a property right existed.[222] Was there "an interest capable of precise definition"? Yes, the court said. "Like a share of corporate stock or a plot of land, a domain name is a well-defined interest."[223] Was the interest "capable of exclusive possession or control"? A domain name was.

---

215. *Dorer*, 60 F.Supp.2d at 561–62.

216. *Umbro*, 529 S.E.2d at 86.

217. *Id.*; *see also* George Vona, Comment, *Sex in the Courts:* Kremen v. Cohen *and the Emergence of Property Rights in Domain Names*, 19 INTELL. PROP. J. 393, 408 (2006) ("[*U*]*mbro* does not stand for the proposition that domain names are not intangible property. In fact, the decision is quite ambiguous."); CRS Recovery v. Laxton, 600 F.3d 1138, 1142-43 (9th Cir. 2010) (declining to interpret *Umbro* more broadly than within the context of Virginia garnishment actions).

218. Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003).

219. *Id.* at 1026–28.

220. *Id.* at 1028–29.

221. *Id.* at 1029.

222. *Id.* at 1030.

223. *Id.*

"Someone who registers a domain name decides where on the Internet those who invoke that particular name—whether by typing it into their web browsers, by following a hyperlink, or by other means—are sent."[224] Finally, did the putative owner "establish[] a legitimate claim to exclusivity"? The court found that domain name ownership was "exclusive in that the registrant alone makes [the] decision" as to where requests for the domain name are sent.[225]

As additional evidence, the Ninth Circuit noted that a robust secondary market exists in which "domain names are valued, bought and sold, often for millions of dollars."[226] Moreover, the court observed, the ACPA provides for *in rem* jurisdiction over domain names where process cannot be served on an alleged cybersquatter, indicating that Congress intended to treat domain names as property.[227] The court therefore concluded that domain names were best characterized as a form of intangible personal property.[228]

But classifying domain names as property did not end the matter. Under the "merger requirement" prescribed by the Restatement (Second) of Torts, a conversion claim for intangible property can be stated only if the intangible property rights converted are "of the kind customarily merged in a document."[229] In reversing the trial court, the Ninth Circuit nonetheless found that California "does not follow the *Restatement*'s strict requirement that some document must actually represent the owner's intangible property."[230] Alternatively, the court reasoned that even if California retained some vestigial merger requirement, it could be satisfied by looking to the DNS itself as the relevant—albeit, electronic—document in which a domain name registrant's rights are merged.[231] The court therefore held that the plaintiff had "an intangible property right in his domain name and that a jury could find that Network Solutions 'wrongfully disposed of' that right to his detriment by handing the domain name over" to another party.[232]

---

224. *Id.*
225. *Id.*
226. *Id.*
227. *Id.*
228. *Id.*
229. *Id.* at 1030–31; RESTATEMENT (SECOND) OF TORTS § 242 (1965).
230. *Kremen*, 337 F.3d at 1033.
231. *Id.* at 1033–35.
232. *Id.* at 1030.

C. *Shakeout and the Merger Requirement*

1. Other Courts

Since *Kremen*, U.S. courts have generally sided with the view that domain names are personal property rather than mere contractual rights.[233] Other jurisdictions to follow the *Kremen* approach include Texas,[234] Utah,[235] Minnesota,[236] Louisiana,[237] Pennsylvania,[238] Florida,[239] and the District of Columbia.[240] U.S. courts have found domain names to be assets in bankruptcy,[241] and, *contra* the result in *Umbro*, some courts have permitted creditors to seize domain names under garnishment, attachment, or other forms of execution.[242]

Courts outside of the U.S. have followed suit. Canada[243] and Sweden[244] have explicitly recognized domain names as property. Judges in at least two UK cases implicitly recognized domain names as property but did not decide squarely on the issue.[245] However, just after those decisions were handed down, the EU Court of Human Rights expressly held that domain names are "property rights" under Protocol No. 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms, thus

---

233. *See* CRS Recovery v. Laxton, 600 F.3d 1138, 1143 (9th Cir. 2010) (noting "'the majority of states' justifiable coalescence around understanding domain names as intangible property").

234. *See* Emke v. Compana, 2007 WL 2781661, at *5 (N.D. Tex. Sep. 25, 2007).

235. *See* Jubber v. Search Mkt. Direct, Inc. (*In re* Paige), 413 B.R. 882, 918 (Bankr. D. Utah 2009).

236. *See* Sprinkler Warehouse v. Systematic Rain, 880 N.W.2d 16, 22 (Minn. 2016).

237. *See* Schott v. McLear (*In re* Larry Koenig & Assoc., LLC), 2004 Bankr. LEXIS 2311, at *21 (Bankr. M.D. La. 2004).

238. *See* Panda Herbal Int'l, Inc. v. Luby (*In re* Luby), 438 B.R. 817, 829-30 (Bankr. E.D. Pa. 2010).

239. *See* St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, No. 806-cv-223-T-MSS, 2006 WL 8442534, at *8 (M.D. Fla. 2006).

240. *See* Xereas v. Heiss, 933 F. Supp. 2d 1, 6-7 (D.C. Cir. 2013).

241. *See, e.g.*, Jubber v. Search Mkt. Direct, Inc. (*In re* Paige), 413 B.R. 882, 918 (Bankr. D. Utah 2009) (domain name as asset in bankruptcy proceeding); Schott v. McLear (*In re* Larry Koenig & Assoc., LLC), 2004 Bankr. LEXIS 2311, at *21 (Bankr. M.D. La. 2004); *In re Luby*, 438 B.R. 817; *see also generally* Alexis Freeman, *Internet Domain Name Security Interests: Why Debtors Can Grant Them and Lenders Can Take Them in This New Type of Hybrid Property*, 10 AM. BANKR. INST. L. REV. 853, 873 (2002).

242. *See, e.g.*, OnlinePartners.com v. Atlanticnet Media Corp., 2000 US Dist. LEXIS 783 at *26, *30–31 (N.D. Ca. 2000) (attachment); Office Depot Inc. v. Zuccarini, 596 F.3d. 696 (9th. Cir. 2010) (execution); Sprinkler Warehouse v. Systematic Rain, 880 N.W.2d 16, 22 (Minn. 2016) (garnishment).

243. *See* Tucows.com v. Lojas Renner S.A., 2011 CanLII C52972 (Can. Ont. C.A.).

244. *See PirateBay.se*, 49 INT'L REV. INTELL. PROP. & COMP. L. 992, 993–94 (2018) (summarizing and translating the decision of the Sweden Supreme Court in the "Pirate Bay" case (No. B 2787-16)).

245. *See* Plant v. Service Direct, [2006] EWCA (Civ) 1259 (appeal taken from Eng.); OBG Limited v. Allan, [2007] UKHL 21 (appeal taken from Eng.).

arguably setting policy for all of Europe.[246] Courts in India[247] and Australia[248] have also implicitly recognized domain names as property.[249]

2. Merger Requirement

But recognizing domain names as property does not, by itself, protect registrants from interference by other parties. As described above in connection with *Kremen*, because conversion is a common law cause of action, whether a registrant may prevail on a claim for conversion of a domain name also depends on whether the forum state adheres to the merger requirement and, if so, whether a domain name can satisfy that requirement. While the *Kremen* court found that California does not follow the merger requirement or, if it does, that the DNS itself qualifies as the requisite document, other jurisdictions have not had such lax attitudes toward the rule.

In *Xereas v. Heiss*, the U.S. District Court for the District of Columbia, after finding domain names to be a form of intangible property, nonetheless dismissed a plaintiff-registrant's claim for conversion of his domain name by his former business partners after strictly applying the merger rule.[250] In *Hoath v. Connect*

246. *See* Paeffgen GmbH v. Germany, Eur. Ct. H.R., 8–9 (2007).

247. *See* Satyam Infoway v. Siffynet Solution (2004) 2 SCR. 465 (India).

248. *See* Hoath v. Connect Internet Services [2006] NSWSC 158 (Austl.).

249. Given overwhelming support in the caselaw for the property status of domain names, it bears examining whether any case has squarely held otherwise that remains good law. With respect to *Dorer* and *Umbro*, both decided under Virginia law, a subsequent decision by the U.S. District Court for the Eastern District of Virginia suggested that if presented with a simple conversion claim for a domain name (not a *fieri facias* or garnishment proceeding), the Virginia Supreme Court would likewise recognize domain names as personal property. *See* E.I. du Pont de Nemours and Co. v. Kolon Indus., 2011 WL 4625760, at *5 (E.D. Va. 2011) ("[A] decision to limit conversion to tangible property or intangible property merged in a document symbolizing ownership would leave domain name users . . . unable to use an action for conversion for substantial interference with their rights. . . . [A]nd this Court concludes that, if confronted with the issue, the Supreme Court of Virginia also would permit a conversion action for converted intangible property . . . ."). *But see* Alexandria Surveys, LLC v. Alexandria Consulting Group, LLC (*In re* Alexandria Surveys Int'l, LLC), 500 B.R. 817, 822 (E.D. Va. 2013) (citing *Umbro* favorably for the proposition that "a judgment debtor has no property right in its telephone numbers and web address"). Although an Appellate Division of the New York Supreme Court did recently deny a straightforward claim for conversion of a domain name on the ground that domain names are not property, *see* NextEngine Ventures v. Network Sols., No. 153341/17, 2017 WL 4569679 (N.Y. Sup. Ct. Oct. 13, 2017), that case was based on an earlier decision that may no longer be good law; *See* Salonclick v. SuperEgo Mgmt., 2017 WL 239379 (S.D.N.Y. Jan. 18, 2017) (reaching the opposite result and opining that a case relied on by *NextEngine Ventures* is no longer good law).

250. Xereas v. Heiss, 933 F. Supp. 2d 1, 7 (D.C. Cir. 2013) ("Xereas does not allege that his property interest were merged in any tangible documents which were transferred to the defendants [and therefore] has failed to show that his claim . . . for conversion states a cognizable cause of action.").

Internet Services Property, Ltd., the Supreme Court of New South Wales denied a plaintiff's conversion claim for theft of his domain name because Australia not only follows the merger rule but further requires the plaintiff to own or control the very document or object in which the intangible right is merged.[251] In the court's judgment, that object was an actual server operated by the .AU registry operator, an even stricter form of the rule.[252] A strictly applied merger rule, therefore, may present a registrant with the bewildering situation in which her domain name is recognized as property and yet she is powerless to protect that property from theft or interference.

It should be noted that rejecting a conversion claim, whether on account of the merger rule or for other reasons, will not always leave a plaintiff-registrant without a remedy for the theft of her domain name. Where a cause of action for conversion has been unavailable, some courts have entertained claims for fraud.[253] Moreover, the ACPA and UDRP remain avenues for relief where a colorable claim of trademark infringement accompanies the actions of an alleged domain name thief.[254] In many cases, these causes of action may suffice to make the aggrieved plaintiff-registrant whole. But facts to support these other claims may not be present in all situations. And, importantly for cases involving DNS censorship, none of the aforementioned causes of action would likely be available where a DNS intermediary seizes a registrant's domain name pursuant to a contractual right.

D. Resolving the Debate

Although the status of domain names as property has become the consensus view, both in the United States and abroad,[255] it bears taking a fresh look at the issue for at least two reasons. First, a number of DNS intermediaries—both registrars and registry operators—still include terms in their agreements requiring registrants to disclaim any property rights in domain names they register.[256] Second, and closely related, courts and scholars who

---

251. *Hoath, supra* note 248, at ¶¶ 135–39.

252. *Id.*

253. *See, e.g.*, CRS Recovery v. Laxton, 600 F.3d 1138, 1145–46 (9th Cir. 2010).

254. *See, e.g.*, *Xereas*, 933 F. Supp. 2d at 14–17 (entertaining a claim under the ACPA for theft of a domain name by a business partner).

255. *See* JONATHAN D. HART, INTERNET LAW 120 (2008) ("[C]ourts generally hold that domain names are subject to the same laws as other types of intangible property.").

256. *See, e.g.*, *Registrant Agreement 2.0*, CAN. INTERNET REGISTRATION AUTHORITY (CIRA), § 3.2, (Oct. 12, 2010), https://cira.ca/registrant-agreement [https://perma.cc/YAZ3-BDUN] [hereinafter CIRA Registrant Agreement 2.0] ("The Registrant acknowledges and agrees that a Domain Name is not property and that a

have previously analyzed the property status of domain names have not done so in the context of domain takedowns by DNS intermediaries. Previous analysis, therefore, concerns only the rights of a registrant over and against third parties who were not parties to any registration agreement.[257] By contrast, a DNS intermediary that seizes a registrant's domain name will, in most cases, act pursuant to a purported contractual right to do so. If a registrant would use property rights to protect herself against such actions, the status of her domain name as property must be sufficiently compelling to overcome any terms in her registration agreement that state otherwise.

In the following sections, I recap some of the stronger arguments for recognizing property rights in domain names. Then, leveraging the technical concepts explained in Part I, I elucidate the precise dividing line between the property nature of domain names and the domain-related services provided by DNS intermediaries, an issue that has at times confused courts and commentators alike.

1. Property Theory

Although no single, canonical definition of property exists, a common formulation holds that property comprises three fundamental rights: the right to use, the right to exclude, and the right to transfer.[258] Within this trio, it is commonly accepted that the right to exclude is the most important and distinctive characteristic of property.[259] It is this element of exclusion that Lord Blackstone referred to in his oft-quoted description of property as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."[260]

Domain names meet all three criteria. Registering a domain name permits the registrant to use the domain by directing all DNS

Domain Name Registration does not create any proprietary right for the Registrant . . . .").

257. To be sure, registrants have asserted conversion claims against registrars previously. *See, e.g.*, Kremen v. Cohen, 337 F.3d 1024, 1035 (9th Cir. 2003); NextEngine Ventures v. Network Solutions, No. 153341/17 LEXIS 3913, at *12 (N.Y. Sup. Ct. 2017). However, in *Kremen*, no contract governed the plaintiff's registration of the domain name at issue. In *NextEngine Ventures*, because the court concluded that New York did not recognize domain names as property, it found no reason to analyze any provisions in the parties' registration agreement.

258. *See* Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 776 (2003).

259. *See* Kaiser Aetna v. U.S., 444 U.S. 164, 176 (1979) (observing that the right to exclude others is one of the "most essential sticks in the bundle of rights that are commonly characterized as property").

260. 2 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 2 (Univ. of Chi. Press 1979) (2d ed. 1766).

requests for it to her website. That right is, by definition, exclusive. As the registrant, Microsoft alone determines, for example, that all requests to MICROSOFT.COM should be directed to Microsoft's website and never to another site. Finally, domain names are freely transferable. As the *Kremen* court noted, a robust secondary market exists in which domain names are frequently bought and sold for millions of dollars. By contrast, secondary markets typically do not exist for rights under consumer service contracts, such as the satellite television service contract hypothesized by the *Umbro* court.

Another important distinction between property rights and contract rights, as pointed out by Anupam Chander, lies in the identity of the individual against whom a right can be asserted:

> If the right can be asserted solely against the contractual counterparty, then the right should properly be declared to be contractual. If the right can be asserted against third parties not in privity with the holder of that right, then it seems appropriate to consider characterizing the right as a property right, even if contract rights may also be involved. Unlike contracts, property gives one rights against third parties.[261]

Under this framework, domain names clearly align with property rights rather than contractual rights. If domain names constituted only contractual rights, registering a domain name would restrict only the contracting registrar from using the name or offering it to another customer. But the promise inherent in registering any domain name is that the same name may not be registered or used in a DNS setting by *any* other party in the world, irrespective of whether that person is a contractual counterparty. In fact, as discussed further *infra*,[262] the rights conferred in a domain name registration transcend the registrant-registrar contractual relationship in other ways, since a registrant may easily transfer a registered domain name from one registrar to another registrar. And even other registry operators may not offer the same domain to other registrants. ICANN's delegation of each top-level domain to a single registry operator ensures that each domain name remains globally unique across the entire DNS. These characteristics of domain names provide exclusive rights

261. Chander, *supra* note 258, at 774. *See also* John Chipman Gray, *Future Interests in Personal Property*, 14 HARV. L. REV. 397, 399 ("Property is a right *in rem* (or against all the world) . . . .").

262. *See supra* Part III.E.3.

beyond the registrant-registrar relationship and even the registrant-registry relationship.

2. Federal Support

Federal laws also support classifying domain names as property. As courts and commentators alike have noted, in cybersquatting cases, the ACPA provides for *in rem* jurisdiction over domain names where the defendant domain name owner cannot be served with process in the United States.[263] Because *in rem* jurisdiction permits a court to exercise jurisdiction over an item of real or personal property based on the fact that the property is located within the jurisdiction, the ACPA evidences Congress's intent to treat domain names as property.[264] Also, Chander notes, the remedy against a cybersquatter under both the ACPA and the UDRP is to transfer the domain name to its "rightful owner"—a property rule.[265]

The PRO-IP Act, another piece of federal legislation, lends additional credence to this notion.[266] Under the PRO-IP Act, as interpreted and executed by the Department of Homeland Security, domain names may be, and have been, seized by federal agents and subject to forfeiture when used in conjunction with websites that host infringing content.[267] The PRO-IP Act, thus, acts as a civil asset forfeiture statute for cybercrimes and, in doing so, treats domain names as property.[268]

3. Service Separability

Some have argued that domain names should not be characterized as property because they are not separable or

263. 15 U.S.C. § 1125(d)(2)(C) (2012).

264. *See also* Tucows.com v. Lojas Renner S.A., 2011 CanLII C52972, ¶¶ 67–72 (Can. Ont. C.A.) (finding a domain name to be "located" in Canada on the basis of registration with a Canadian registrar for purposes of exercising personal jurisdiction over a Brazilian company).

265. Chander, *supra* note 258, at 777.

266. *See generally* Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256 (codified at 18 U.S.C. § 2323) (2012).

267. *Id.*; *see* OFFICE OF MGMT. & BUDGET, U.S. INTELL. PROP. ENF'T COORDINATOR, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 65 (2013) (indicating the seizure of more than 1,700 domain names under the act); *see also* Annemarie Bridy, *Three Notice Failures in Copyright Law*, 96 B.U. L. REV. 777, 796–97 (2016) (detailing the federal government's interpretation of the PRO-IP Act to permit domain name seizure).

268. *See* Annemarie Bridy, *Carpe Omnia*, *supra* note 193, at 688 ("Civil forfeiture, by contrast, operates *in rem* and is justified by the legal fiction that the property itself is guilty of wrongdoing and therefore subject to confiscation.").

independent from the services provided by DNS intermediaries.[269] As first articulated in *Dorer*, a domain name registration is the "product of a contract for services" between the registrar and the registrant.[270] By itself, this statement does little to advance a contract rights theory of domain names. Service contracts often give rise to property rights. Examples include freelance developers hired under contract to build software products or a patron who commissions a work of art. Instead, what the *Dorer* court likely meant was better articulated by the Virginia Supreme Court in *Umbro*, which stated, "whatever contractual rights the judgment debtor has in the domain names at issue in this appeal, those rights do not exist separate and apart from [Network Solutions'] services that make the domain names operational Internet addresses."[271] Or, even more to the point, "[the registrant's] contractual right is *inextricably bound* to the domain name services that [Network Solutions] provides."[272]

However, both statements misconstrue the role of registrars, such as Network Solutions, in the operation of a domain name. As explained *supra*, registrars perform no core DNS services necessary to make domain names operational.[273] A registrar's role is largely limited to taking payment for a domain name registration or renewal, instructing the relevant registry operator to register the domain name and authoritative nameservers in the registry database and zone file, and notifying the registrant of upcoming renewal deadlines. These functions, all of which may be classified as merely administrative or clerical, are not necessary for a domain name to function in connection with a website. If a customer registers a domain name for the maximum ten-year registration period and pays all necessary fees upfront, the domain can continue to operate uninterrupted for the full ten-year period, even if the registrar stops providing services or goes out of business altogether.[274]

---

269. *See, e.g.*, *Registration Agreement*, *supra* note 137, at § 5 ("You further agree that domain name registration is a service, that domain name registrations do not exist independently from services provided pursuant to this or a similar registration agreement with a registrar, and that domain name registration services do not create a property interest."); Sheldon Burshtein, *Is a Domain Name Property?*, 1 J. INTELL. PROP. L. & PRAC., 59, 61 (2005) ("[T]he continued right to use . . . a domain name is dependent on the continuation of services from the . . . domain name registry.").

270. Dorer v. Arel, 60 F. Supp. 2d 58, 561 (1999).

271. Network Solutions v. Umbro, 529 S.E.2d 80, 86 (2000).

272. *Id.* (emphasis added).

273. *See supra* Part I.

274. Although some registrants may rely on their registrars to operate authoritative nameservers, which *are* essential to the resolution of their domain names (Steps 6 and 7 in Fig. 1), a registrant may contract with any capable service provider to operate

Without doubt, operability of a domain does require that a registry operator—an entity that was not a party in *Dorer* or *Umbro*—provide ongoing service by responding to DNS queries (Steps 4 and 5 in Fig. 1). If the registry operator fails to provide name resolution services, even for a day, the domain name will cease to function. And given the hierarchical nature of the DNS, no other entity may perform this function. Yet, this fact does not disqualify the domain name from property status. To hold that it does is to ignore the bundle-of-sticks nature of property, to conflate the plural attributes of property into a unitary definition. A registry operator's refusal to provide resolution services for a particular domain name would operate to remove only one stick from the registrant's bundle: the right to use—or, perhaps more accurately, the *ability* to use—the domain name. But a domain name is no less property because a registrant depends on a third party to use the domain name, any more than other assets lose their property status when the use right is abridged.

In addition to providing resolution services, a registry operator must also maintain accurate records in its registry database to prevent multiple parties from registering the same domain name. A registrant can remain secure in her right to a domain name only if the registry operator continues to perform these registry services. But the same could be said of other classes of property. A corporation's failure to perform the basic clerical service of maintaining an accurate shareholder registry could endanger the security of shareholders' property rights. But that fact does not take away from the property status of corporate shares, just as a parcel of land does not depend on the continued services of a title office in order to remain property. Record-keeping merely operates to clarify which party can lay superior *claim* to the subject property.

E. Nature of the Property Interest

Having established domain names as a form of personal property, a question naturally arises: what specific rights do registrants have in that property? In particular, the existing literature has been strangely silent on what is perhaps the most important question: does a registrant own her domain name, or does she merely acquire a right to possess it?

As analyzed further *infra*, whether registrants own or merely lease their domain names significantly affects the balance of power

---

nameservers or even perform the function herself. The same cannot be said for satellite television services. *See* Annette Nellen, *Domain Names and Other Intangibles for Internet Business*, 14 J. TAX'N F. INST. 31 (2001).

between registrants and DNS intermediaries.[275] If a registrant merely leases her domain name, then, presumably, her registrar can prescribe enforceable rules for how she may use it in a registration agreement, such as by imposing morality-based content policies or other acceptable use restrictions. By contrast, if a registrant takes title to her domain name when she registers it, courts may be less willing to uphold a registrar's right to seize her property as a self-help remedy for breach.

Not surprisingly, DNS intermediaries have largely remained silent on this issue.[276] To speak of ownership, even to require registrants to disclaim it, could lend credence to the foundational premise that domain names are property—something DNS intermediaries may be reluctant to do. But even if DNS intermediaries took a strong stance on this issue in their contracts, multiple factors support the notion that registrants take title to their domain names upon registration. Those factors include the case law, property theory, and the role of DNS intermediaries, including ICANN, in the global Internet community.

1. Case Law

In addition to recognizing domain names as property, several courts have either explicitly referred to registrants as owners of their domain names or else used language strongly suggestive of ownership. For example, in *Kremen*, the Ninth Circuit referred to the original registrant as "the proud owner of SEX.COM."[277] In *Gill v. American Mortgage Educators, Inc.*, the United States District Court for the Western District of Washington stated, "Domain names are considered to be *owned* by the person who registered the name with the registrar."[278] In *Mold.ca Inc. v. Moldservices.ca Inc.*, the Ontario Superior Court of Justice had occasion to consider a case in which one partner used another partner's money to register various company domain names in his (the first partner's) own name.[279] Dismissing the defendant's argument that the contact

275. *See supra* Part IV.A.

276. *But see Acceptable Use and Takedown Policy*, *supra* note 145 ("As the *owner* of a domain name, you are required to act responsibly in your use of that domain . . . .") (emphasis added); *10 things you absolutely MUST know before you register a domain with anyone*, EASYDNS, § 5, https://easydns.com/10-things-to-know-before-you-register/ [https://perma.cc/2BCN-UND6] (last visited Oct. 18, 2020) ("[I]n the eyes of the domain Registry to which all the Registrars interact, and the Registry's oversight body (like ICANN, or in Canada, CIRA), whoever is listed in the domain WHOIS record as the domain Registrant is the legal owner of the domain name.").

277. Kremen v. Cohen, 337 F.3d 1024, 1026 (9th Cir. 2003).

278. 2007 U.S. Dist. LEXIS 69636, at *14 (W.D. Wash. Sept. 19, 2007) (emphasis added).

279. Mold.Ca Inc. v. MoldservicesCa.Inc., [2013] ONSC Court File No. 480391 (Can. Ont. S.C.).

information used during registration should control, the Court held, "*Title* to the domain names belongs to the corporate plaintiffs."[280] Other courts have used similar language.[281]

Some DNS intermediaries might object to drawing conclusions based on this language alone. In these cases, they might argue, the courts were not called upon to decide whether registrants own their domain names or merely had possessory interests. The courts were instead adjudicating other issues and simply reached for familiar and accessible terminology when describing how certain domain names in dispute were acquired or held. Or, because one can "own" a right in a property (e.g., an exclusive possessory right) without owning the property itself, courts' use of ownership language in *dicta* does not, by itself, mean that registrants own their domain names.

While it is true that some of the cases that used ownership language did not hinge on whether registrants actually held title to their domain names, in other cases, courts relied on property concepts that make little sense outside of an ownership context. For example, in *Express Media Group v. Express Corp.*, a cybercriminal managed to alter the WHOIS information associated with a domain name by replacing the plaintiff-registrant's email address with its own.[282] The defendant, believing it was communicating with the plaintiff, later purchased the domain name from the cybercriminal at a price far below market value.[283] When the plaintiff, which the court described as the "rightful owner" of the domain, sued the defendant for conversion of its domain name, the defendant argued that it was immune to liability under the good-faith purchaser defense.[284] The U.S. District Court for the Northern District of California disagreed, explaining that "[t]he law distinguishes between the person who purchased from someone who obtained title to the property by fraud"—in which case the defense applies—"and the person who purchased from a thief who had no title to

280. *Id.* at 2 (emphasis added).

281. *See, e.g.*, Emke v. Compana, 2007 WL 2781661, at *5 (N.D. Tex. Sep. 25, 2007) ("While the domain name is an intangible thing, the court determines that it is reasonable to find that it was located in California because it was *owned* by Emke.") (emphasis added); CRS Recovery v. Laxton, 600 F.3d 1138, 1143 (9th Cir. 2010) (describing registrants as "purchasers" of domain names); Tucows.com, *supra* note 243, at ¶ 65 (observing that the plaintiff's "ownership of the domain name" had a "degree of permanency" and that the plaintiff had "owned the domain name" for several years); Hoath v. Connect Internet Services [2006] NSWSC 158 (Austl.) (employing ownership language throughout the opinion); *Express Media Grp., LLC v. Express Corp.*, 2007 WL 1394163, at *1 (N.D. Cal. May 10, 2007) ("WHOIS records are maintained by domain name registrars that make domain name contact and ownership information searchable and available to the public.").

282. *Express Media Grp.*, 2007 WL at *1.

283. *Id.* at *2.

284. *Id.* at *5.

sell"—in which case it does not.[285] Because the cybercriminal had merely altered the WHOIS information associated with the domain name, rather than transferring the domain to itself, title never passed to the cybercriminal.[286] The cybercriminal, therefore, could not pass title to the defendant, and the good-faith purchaser defense did not apply.[287]

In *Miles dba Jazz Alley v. Tokaido Shosha*, an employee registered to himself a domain name comprising his employer's trademark, which he later sold to a third party.[288] To gain control of the domain name, his employer filed a cybersquatting claim against the purchaser under the UDRP.[289] Although the respondent-purchaser had not registered the domain name in bad faith when he purchased it from the erstwhile employee, a necessary element to prevail in a UDRP action, the UDRP panel held that "[o]ne cannot pass good title to a domain name where it does not have good title."[290] Thus was born the rule that if a party registers a domain name in bad faith, that bad faith will run with title to the domain name for any future purchaser of the domain, a rule that has been reaffirmed in multiple UDRP proceedings, including proceedings adjudicated by the World Intellectual Property Organization.[291]

These cases turned on chain-of-title and defect-of-title issues, concepts having meaning typically only in transfers of title-held or owned property. In the same manner, the remedies of garnishment and attachment typically require that the debtor own the garnished or attached property.[292] Therefore, it could be said that courts that have allowed creditors to garnish or attach domain names have, by necessary implication, also held that the registrants owned their domain names. It thus becomes more difficult in these decisions and

285. *Id.* at *5.

286. *Id.* at *6.

287. *Id.*; *see also* CRS Recovery v. Laxton, 600 F.3d 1138, 1145–46 (9th Cir. 2010) (conducting a similar analysis as to the quality of title based on whether the contested domain name was obtained by theft vs. fraud); Jubber v. Search Mkt. Direct, Inc. (*In re Paige*), 413 B.R. 882, 919 (Bankr. D. Utah 2009) ("Because Sayers obtained the Domain Name through conversion, he could not pass good title to Timothy or anyone else.").

288. ICANN Administrative Panel Decision, Miles dba Jazz Alley v. Tokaido Shosha, (2000) No. AF-0318 at *1.

289. *Id.*

290. *Id.*

291. *See, e.g.*, Mucos Emulsions, GmbH & Marlyn Nutraceuticals, Inc. v. Esex.org & Kim Taeho, WIPO Case No. D2000-1513 (2001); Van Morrison and Exile Productions Limited v. Unofficial Club de Van Morrison, WIPO Case No. D2002-0417 (2002); Maglificio Gran Sasso Spa v. Info., WIPO Case No. D2004-0019 (2004).

292. *See, e.g.*, A.C.A. Am. Masters, Inc. v. Wertz, 358 N.Y.S.2d 445 (N.Y. App. Div. 1974) ("An attachment of property not belonging to the defendant is without effect and will generally constitute an abuse of discretion"); Consumers United Ins. Co. v. Smith, 644 A.2d 1328, 1352 (D.C. 1994) ("A court's ability to order attachment is limited to the delivery of property that belongs to a judgment debtor but is being held by a third party").

others like them to dismiss the court or panel's language of ownership as mere *dicta*.

2. Property Theory

Property theory also supports the notion that registrants own their domain names. In his famous 1961 essay, "Ownership," Oxford Regius Professor, A. M. Honoré listed and described what he regarded as the eleven incidents of ownership—namely,

> [T]he right to possess, the right to use, the right to manage, the right to the income of the thing, the right to the capital, the right to security, the rights or incidents of transmissibility and absence of term, the prohibition of harmful use, liability to execution, and the incident of residuarity. . . .[293]

Setting aside the prohibition of harmful use, which operates as more of a limitation on use than a positive indicium of ownership, we see that the manner in which registrants hold domain names accords with most or all of these incidents. Upon registering a domain name, a registrant has exclusive possession of the name, having sole authority to determine which IP addresses it maps to.[294] Furthermore, in jurisdictions that recognize claims for the conversion of domain names, courts will order misappropriated domain names to be returned to the exclusive possession of the registrant.[295] Registrants have the right to use their domain names to direct Internet traffic to whichever websites they choose. Registrants have the right to manage their domain names by deciding which employees, contractors, or other parties may use or configure the registration and zone file records for DNS resolution.

Registrants have the right to income from their domain names, either indirectly through revenue from their websites or directly by

293. A. M Honoré, *Ownership*, in PATRICIA SMITH, THE NATURE AND PROCESS OF LAW: AN INTRODUCTION TO LEGAL PHILOSOPHY 370 (Oxford Univ. Press 1993) [hereinafter, Honoré, *Ownership*]. I'm indebted to Konstantinos Komaitis for his previous work analyzing domain names against Honoré's incidents of ownership—*see* KONSTANTINOS KOMAITIS, THE CURRENT STATE OF DOMAIN NAME REGULATION: DOMAIN NAMES AS SECOND CLASS CITIZENS IN A MARK-DOMINATED WORLD 16–17 (Routledge 2010)—and his recommendation to supplement that analysis in this article.

294. *See* DUNCAN SHEEHAN, THE PRINCIPLES OF PERSONAL PROPERTY LAW 7 (2017) ("[T]here is a presumption that the person in possession is the owner, and vice versa." (*citing* Ramsay v. Margerett, [1894] 2 QB 18)).

295. *See, e.g.*, *Express Media Grp., LLC v. Express Corp.*, 2007 WL 1394163, at *10–11 (N.D. Cal. May 10, 2007) ("Defendants are ordered to return the domain name express.com to plaintiffs . . . and to cooperate with plaintiffs in adjusting all registrations and usages so that plaintiffs shall have unfettered use of the name.").

leasing their domain names to third parties.[296] Registrants have the right to capital, which Honoré describes as "the power to alienate [or] consume" the thing, including the power to transfer title upon death.[297] Registrants may sell their domain names to whom they like, and domain names constitute heritable assets in that an owner's death does not terminate the domain registration. The incident of transmissibility, which Honoré describes as the ability of the interest to be "transmitted to the holder's successors and so on *ad infinitum*,"[298] reflects how domain names are held, in that they can be bought and sold through a chain of title that continues indefinitely. At no point, does a domain name reach its maximum number of owners such that it cannot be acquired by the next successor in interest, reverting instead to unregistered status. As for liability to execution, a number of jurisdictions have permitted domain names to be seized from debtors through bankruptcy, garnishment, or attachment.[299] Finally, registrants are the ultimate residuaries when any interests they grant to others short of ownership cease.

With respect to the right to security, which Honoré describes as the right "to remain owner indefinitely,"[300] and the absence of term, satisfying these incidents of ownership is admittedly more complicated. Registrants may register or renew their domains for no more than ten years at a time. Registrants must also pay renewal fees; failure to do so will cause the registration to expire, at which point another party may register the domain name. Still, if we analogize renewal fees to property taxes, we find that their existence is not inconsistent with domain name ownership.

Derived from the feudal concept of socage, in which the king would divide land among his lieutenants and collect a share of their profits in exchange for his protection over the land,[301] property taxes are still used today to fund services that protect private property in the United States, such as police and fire protection.[302]

---

296. *See What is Domain Leasing?*, LENDVO, https://www.lendvo.com/domain-leasing/ [https://perma.cc/3484-52NH] (last visited Oct. 18, 2020) (describing the process by which a domain name may be leased to another party).

297. Honoré, *Ownership*, *supra* note 293, at 372.

298. *Id.* at 373.

299. Juliet Moringiello, *Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future*, 72 U. CIN. L. REV. 95, 103; *see* materials cited, *supra* note 242.

300. Honoré, *Ownership*, *supra* note 293, at 374.

301. Alana Semuels, *The Feudal Origins of America's Most-Hated Tax*, THE ATLANTIC (Aug. 24, 2016), https://www.theatlantic.com/business/archive/2016/08/the-feudal-history-of-property-tax-in-america/497099/ [https://perma.cc/F3T2-2QCN].

302. Hanna Elsaadi, *The Cost of Education: An In-Depth Look into Texas's Education Funding System over the Last Two Decades*, 2 TEX. A&M J. PROP. L. 341, 344 (2015) ("Aside from schools, local property taxes also provide funds for roads, streets, fire protection, and police departments.").

Revenue from property taxes is also used to subsidize infrastructure such as roads, bridges, and drainage.[303] Together, these public functions operate to *protect* and *connect* real property. Moreover, even in fee simple absolute, a property owner's failure to pay property taxes may result in a tax lien and foreclosure, depriving her of title and making the property available to others.[304]

These facts and rationales align nicely with the DNS, wherein DNS intermediaries must perform ongoing services to protect and connect domain name properties. Like county title offices, registry operators maintain authoritative registry databases indicating which registrants own which domain names, thus protecting registrants from competing claims by third parties. Registry and root server operators connect domain names to the global Internet by mapping IP address associations in zone files and responding to DNS queries.

Originally funded by universities and government agencies—with the result that domain names were free until 1995—these services are now funded almost exclusively through registration fees.[305] Like a foreclosure to enforce a tax lien, the specter of domain name expiration serves as an enforcement mechanism to ensure that registration fees are paid so that the broader DNS can continue to operate. Were these functions to be subsidized through other means, domain names could theoretically be held perpetually without the need for renewals or renewal fees.

The notion that limited registration terms derive from the need to collect registration fees to offset DNS operational costs finds support in the administration of IP addresses. Although the legal status of IP addresses is beyond the scope of this article, as with domain names, there is support both for the proposition that IP addresses are a form of property[306] and that entities may own their address blocks.[307] Unlike domain names, however, IP addresses,

303. Chad D. Emerson, *All Sprawled Out: How the Federal Regulatory System Has Driven Unsustainable Growth*, 75 TENN. L. REV. 411, 430 (2008).

304. *See, e.g.*, Lee Anne Fennell, *Fee Simple Obsolete*, 91 N.Y.U. L. REV. 1457, 1470 n.49 (2016) ("An owner's possession of her property can be truncated involuntarily by failing to pay her mortgage or property taxes.").

305. *See The Internet Grows Up*, *supra* note 85 (replacing NSF funding with registration fees as the primary vehicle for funding operation of the DNS).

306. *See* In re Nortel Networks Inc., 2011 WL 1560720 (Bankr. D. Del. Mar. 21, 2011) (recognizing IP addresses as assets in bankruptcy); *Cf.* Ernesto M. Rubi, *The IPV4 Number Crisis: The Question of Property Rights in Legacy and Non-Legacy IPV4 Numbers*, 39 AIPLA Q.J. 477, 478 (2011).

307. *See* Letter from NSF General Counsel, Lawrence Rudolph, (Aug. 30, 2012), available at https://via.hypothes.is/https://www.internetgovernance.org/wp-content/uploads/NSF_GC_Letter_RE_ARIN.pdf [https://perma.cc/PW9L-99SE]

once procured, can be held perpetually.[308] Address block holders need not renew their IP addresses or pay ongoing fees in order to maintain their blocks.[309]

This distinction between perpetually held IP addresses and merely renewable domain names is no doubt explainable by the fact that IP addresses operate in a decentralized manner. Unlike, a domain name, which depends on one of thirteen root server operators and a single registry operator to resolve, an IP address does not depend on any central authority to ensure that Internet traffic bound for the address reaches the appropriate host. Instead, through a complex web of peering agreements and the border gateway protocol (BGP), ISPs and Internet backbone operators together ensure that IP addresses remain under the exclusive control and use of their owners. The costs of protecting and connecting IP addresses are, thus, subsumed within the broader network connectivity and peering market. Were the DNS to operate in a similar decentralized manner in which the costs of operation were borne by network operators, as some scholars have proposed,[310] recurring registration fees could be done away with

(affirming that that a legacy IPv4 address block holder owned its addresses and that the American Registry for Internet Numbers (ARIN), the organization responsible for allocating IP addresses in North America, has no power to reclaim the block) [hereinafter, NSF LETTER]; Milton Mueller, *It's official: Legacy IPv4 Address Holders Own their Number Blocks*, INTERNET GOVERNANCE PROJECT (Sep. 22, 2012), https://www.internetgovernance.org/2012/09/22/its-official-legacy-ipv4-address-block-holders-own-their-number-blocks/ [https://perma.cc/Q6W9-WCL3]; Rubi, *supra* note 306 ("By finding that Nortel had all of the rights appurtenant to property ownership in its legacy IPv4 numbers, the court paved the way for future bankruptcy debtors to treat IPv4 numbers as assets that can be offered for sale."). *Cf.* Chism v. Washington, 683 F. Supp. 2d 1145, 1148 (E.D. Wash. 2010), *rev'd sub nom.* Chism v. Washington State, 655 F.3d 1106 (9th Cir. 2011), *withdrawn from bound volume and rev'd and remanded*, 661 F.3d 380 (9th Cir. 2011) ("The IP address (68.113.11.49) was owned by Charter Communications.").

308. See NSF LETTER, *supra* note 307. In this, I refer not to Internet users, who may be temporarily assigned different IP addresses by their Internet service providers each time they connect, but to organizations that obtain blocks of IP addresses from a Regional Internet Registry.

309. It should be noted that for a subset of IPv4 addresses known as "non-legacy" addresses, ARIN does require block holders to pay annual fees. *See Fee & Billing Information*, AM. REGISTRY FOR INTERNET NUMBERS, https://www.arin.net/resources/fees/ [https://perma.cc/7TMS-4DC8] (last visited Oct. 18, 2020). However, because ARIN does not play an operational role in how Internet traffic is routed to IP addresses, these fees go primarily toward maintaining public records of IP address allocation. Some scholars have questioned the value of the services provided by ARIN and other regional registries and suggested that contractual requirements to pay such fees may even been unenforceable. *See, e.g.*, Rubi, *supra* note 306, at 495.

310. *See, e.g.*, Matthias Wachs, Martin Schanzenbach & Christian Grothoff, *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*, CRYPTOLOGY & NETWORK SECURITY 127 (2014).

and the enforcement mechanism of domain name expiration along with it.[311]

Still another rationale for renewal fees might be to promote the efficient use of domain names by ensuring that valuable names do not lie fallow on account of registrants who register and then neglect them. This too accords with one of the classic rationales for property taxes.[312] It may provide a further reason why IP addresses, which, unlike domain names, are essentially fungible, have not been subject to renewal fees.

Accordingly, when viewed through the lens of property taxes, the requirement that registrants continue to pay renewal fees, or else risk losing their domain names, is not antithetical to the right-to-security and absence-of-term incidents of ownership. Property taxes present similar burdens and title risks to holders of fee simple estates, and yet few would argue that such estate holders do not own their properties as a result.[313]

In any event, even if these particular incidents are not met, their absence alone does not vitiate registrants' claim to title.[314] Indeed, other forms of intellectual property in the United States have limited terms and/or require the owner to pay maintenance or renewal fees. Patent terms are limited to twenty years[315] and may be cut short by an assignee's failure to pay maintenance fees after issuance.[316] Copyrights have limited terms, and under the 1909 Copyright Act, prior to its replacement in 1976, copyright holders were required to pay a renewal fee to extend their registrations for

311. In fact, unofficial .ONION domain names, which are operationalized through a decentralized peer-to-peer network, already carry no renewal fees. *See Pricing*, PEERNAME, https://peername.com/pricing/ [https://perma.cc/2S47-CSMQ] (last visited Oct. 18, 2020) (providing no renewal fee for .ONION domain names).

312. *See* Semuels, *supra* note 301, ("All of the 13 original colonies' charters stated that land be held in free and common socage. This motivated entrepreneurial colonists to make sure they could make money on their land . . ."); *accord* Eric Posner & E. Glen Weyl, *Property is Only Another Name for Monopoly*, 9 J. LEGAL ANALYSIS 51, 95–97 (2017) (proposing a supplemental system of governmental taxation on domain names to ensure their efficient allocation among interested parties).

313. *Cf.* Frederick M. Abbott, *On the Duality of Internet Domain Names: Propertization and Its Discontents*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 1, 23 (2013) ("A domain name effectively has an indefinite duration and is durable [contingent on the payment of renewal fees], which is more characteristic of property than typical contract rights").

314. *See* Honoré, *Ownership*, *supra* note 293, at 370 ("[T]he use of 'owner' will extend to cases in which not all the listed incidents are present."); *see also* People v. Walker, 33 Cal. App. 2d 18, 20 (Cal. 1939) ("[T]he pruning away from some or a great many of these elements does not entirely destroy the title.").

315. 35 U.S.C. § 154(a)(2) (2018) (limiting a utility patent's term to twenty years from the earlier of the patent application filing date or the earliest application to which the patent claims priority).

316. 35 U.S.C. § 41(b) (2018).

a second twenty-eight-year term.[317] Similar to the maximum ten-year registration period for domain names, holders of registered trademarks must submit a Declaration of Use and Renewal and pay the accompanying renewal fee every ten years to maintain their trademarks.[318] Despite the limited terms or renewal fees associated with these categories of intellectual property, few would argue that holders of patents, copyrights, or trademarks do not own their intellectual property.

3. No Better Claimant to Title

If DNS intermediaries would argue that registrants do not hold title to their domain names, then they must establish which party does hold title.[319] It will not do simply to characterize registrants as lessees of their domain names; one must identify the lessor. If title does not lie with registrants, then four other candidates emerge: registrars, registry operators, ICANN, and the global Internet community. I now analyze whether any of these entities may have a better claim to title.

If a registrant merely leases her domain name, then her registrar becomes an obvious candidate for lessor. After all, registrants pay and contract with registrars directly for their domain names. Registrants appear to receive their domain names from registrars, and registrars claim the right to revoke registrations under the terms of their registration agreements. However, a registrar's similarity to a lessor ends there, and at least three facts weigh strongly against characterizing registrars as the owners of registered domain names.

First, prior to registration, no registrar has a superior claim to a domain name over any other registrar. The registrant who chooses to register EXAMPLE.COM may select from any registrar authorized to offer .COM domain names. If the registrant merely leases her domain name from her registrar, then the registrar must somehow acquire the domain name from another party (e.g., the registry operator) at the time of registration in order to simultaneously lease it to the registrant. No evidence suggests this happens. ICANN refers to registrars as mere "sponsors" of domain names registered through them,[320] and some registry operators

317. *See* Copyright Act of 1909, 17 U.S.C. § 1(d) (1970), *repealed by* Copyright Act of 1976, Pub. L. No. 94-553, § 101, 90 Stat. 2541.

318. 15 U.S.C. § 1059(a) (2018).

319. Lacey Nursing Ctr., Inc. v. Dep't of Revenue, 103 Wash. App. 169, 177 (2000) ("The term property is commonly used to denote everything which is the subject of ownership . . . .") (quoting BLACK'S LAW DICTIONARY at 1216)).

320. *See Registrar Accreditation Agreement*, ICANN, §§ 1.16, 3.2.2, 3.4.1 (Aug. 2, 2012), https://www.icann.org/resources/pages/ra-agreement-2009-05-21-en [https://perma.cc/44RJ-E8R3].

expressly state that registrars acquire no proprietary interests in registered domain names.[321] Nor do any registrars appear to lay claim to title for registered domain names anywhere in their registration agreements. While some registrars disclaim any proprietary right to domain names on behalf of the registrant, they do not go further by claiming that *they* own such proprietary rights.

Second, registrants are free to transfer their domain names between registrars pursuant to ICANN's Inter-Registrar Transfer Policy.[322] If registrars hold title to registered domain names, then transferring a domain name from one registrar to another would necessarily entail a transfer of title between the two registrars, complete with consideration and a deed of conveyance of some sort. Again, no evidence suggests this happens. No money flows from the losing registrar to the receiving registrar during a domain name transfer, and registrars do not enter into any contracts or deeds of conveyance with each other. Moreover, it would indeed be a strange phenomenon in property law if a lessee had the unilateral power to swap out her lessor and force a conveyance of her leased property between third parties at any time.

Finally, when a domain name registration expires, the domain name reverts not to the sponsoring registrar but to the registry operator for the top-level domain. And, once reverted, anyone can register the domain name through any accredited registrar. If registrars own all registered domain names, one would expect all rights to a domain name to revert to the sponsoring registrar when the registration expires. This does not happen. Instead, if the sponsoring registrar wishes to use an expired domain name for its own purposes, it must register the domain name like any other registrant; it must even compete with professional drop-catchers in the race to snatch the domain name once it becomes available.[323] Together, these facts show that whatever property role registrars assume in the registration of a domain name, it is not the role of a lessor, and thus registrars cannot be said to own the domain names registered by their customers.[324]

---

321. *See, e.g.*, CIRA Registrant Agreement 2.0, *supra* note 256, at § 3.2 ("[A] Domain Name Registration does not create any proprietary right for the Registrant, *the Registrar of Record* or any other person in any name used as a domain name or in any Domain Name Registration." (emphasis added)).

322. *See Transfer Policy*, *supra* note 61.

323. *SEE* MIRAMIRKHANI ET AL., *supra* note 67, at 1 (noting that some registrars invest millions of dollars in infrastructure to catch valuable domains at the exact moment they become available).

324. *See also* Express Media Grp., LLC v. Express Corp., 2007 WL 1394163, at *9 (N.D. Cal. May 10, 2007) ("Nothing in the facts or the agreement would indicate that [the registrar] ever held title. Plaintiffs registered their domain name with Network Solutions, but they did not pass title to it.").

Given that a domain name reverts to the relevant registry operator when a registration expires, registry operators represent the next logical candidate for title-holder. Yet, registry operators, like registrars, do not claim to own domain names within the top-level domains they manage, and some registry operators expressly disclaim any proprietary interest in second-level domains.[325] Nor do registry operators claim registered or unregistered assets in their financial statements.[326] Moreover, as with registrars, if a registry operator wishes to use a domain name for its own purposes, it must register the domain name through an ICANN-accredited registrar just like any other registrant.[327] It is not permitted to use an unregistered domain name in any manner it chooses, as would be expected of a typical property owner whose property is not under lease.

While there may be some merit to the argument that registry operators have a residuary interest in expired domain names, they too could be dispossessed of any such interest if ICANN were to re-delegate management of the top-level domain to another entity. It is perhaps for this reason that ICANN has vigorously asserted in litigation that country code top-level domain managers do not own the top-level domains they manage.[328] If ICANN were to re-delegate management of the .BIZ top-level domain, for example, from NeuStar, Inc. to another entity,[329] NeuStar would necessarily

---

325. *See* Tingsratt [TR] [District Court] 2015 B 6463-13 (Swed.), https://internetstiftelsen.se/docs/Stockholms-TR-B-6463-13-Deldom-2015-05-19_avidentifierad.pdf [https://perma.cc/CSA5-3F8J] (noting that the Foundation for Internet Infrastructure, the operator of the .SE top-level domain, expressly disclaimed any proprietary interest in the PIRATEBAY.SE and THEPIRATEBAY.SE domain names that were registered to a customer).

326. *See* 2018 ANNUAL REPORT, VERISIGN 46 (2018), https://investor.verisign.com/static-files/e8779668-99cc-40b9-99ed-bd38dd6c33f9 [https://perma.cc/E3GE-JRNG] (claiming "Other current assets"—excluding cash, securities, and property—of $47 million, an amount that fails to exceed the market value of even certain individual domain names, let alone the aggregate value of all .COM domain names); *See, e.g.*, Michael Berkens, *Report: Vegas.com Bought LasVegas.com in 2005 For Up To $90 Million Dollars*, THEDOMAINS (Nov. 6, 2015), https://www.thedomains.com/2015/11/06/report-vegas-com-bought-lasvegas-com-in-2005-for-up-to-90-million-dollars/ [https://perma.cc/2G2L-BMMU] (reporting on the sale of LASVEGAS.COM for $90 million).

327. *Base Registry Agreement,* ICANN, *supra* note 73, at § 2.6 ("[I]f Registry Operator is the registrant for any domain names in the registry TLD, such registrations must be through an ICANN accredited registrar....").

328. Memorandum in Support of ICANN's Motion to Quash at 13–16, Rubin, et al. v. Islamic Republic of Iran, et al., Case No. 01-1655-RMU (D. D.C. Sept. 29, 2014) [hereinafter ICANN's Brief]. While ICANN's statements were confined to top-level domains, rather than second-level domains, the same logic would no doubt hold for all domain names within the top-level domains managed by registry operators.

329. *See Registry Listings*, ICANN, https://www.icann.org/resources/pages/listing-2012-02-25-en [https://perma.cc/MN29-VTZF] (last visited Oct. 18, 2020) (listing NeuStar as the registry operator for the .BIZ top-level domain).

lose control of all .BIZ second-level domain names. By contrast, if NeuStar owns all .BIZ domain names, it could not be so easily dispossessed of such property by another entity without compensation.

If registry operators do not own domain names under their management, then perhaps it follows that title ultimately rests with ICANN. After all, ICANN has the power to deprive a registry operator of a top-level domain through re-delegation and therefore has a stronger residuary interest than registry operators, registrars, or registrants. Still, this theory suffers from some of the same problems that arise when analyzing other DNS intermediaries' claims to ownership.

First, under this reasoning, ICANN would hold title not only to all domain names within a particular top-level domain but to all domain names in all top-level domains—effectively, all domain names in the world. If true, such an extensive asset base would make ICANN one of the most valuable private corporations in the world. One method for appraising already-registered domain names involves measuring the daily unique visitors, unique pageviews, and revenue from advertisements of the website associated with the domain name. Using these and other factors, one appraisal tool estimates the value of GOOGLE.COM at $2.25 billion;[330] BAIDU.COM, the most popular search engine in China, at $560 million;[331] and FACEBOOK.COM at $740 million.[332] The market value of these three domains alone dwarfs the $514 million in assets listed in ICANN's latest financial report.[333]

Not surprisingly, ICANN has never asserted ownership of third-party domain names, which explains the absence of any domain name assets from its financial statements. In part, ICANN's failure to claim ownership of domain names may stem from a policy position that would classify domain names as contract rights rather than property.[334] The more likely reason is that

330. *Google.com Traffic Worth*, SITEWORTHTRAFFIC, http://www.siteworthtraffic.com/report/google.com [https://perma.cc/G6BJ-YRNN] (last visited Oct. 18, 2020).

331. *Baidu.com Traffic Worth*, SITEWORTHTRAFFIC, http://www.siteworthtraffic.com/report/baidu.com [https://perma.cc/Y7AQ-VJA7] (last visited Oct. 18, 2020).

332. *Facebook.com Traffic Worth*, SITEWORTHTRAFFIC, http://www.siteworthtraffic.com/report/facebook.com [https://perma.cc/VKW8-RXGM] (last visited Oct. 18, 2020).

333. *See* 2019 ANNUAL REPORT, ICANN 45 (2019), https://www.icann.org/en/system/files/files/annual-report-2019-en.pdf [https://perma.cc/8ALW-CT8W].

334. *See* ICANN's Brief, *supra* note 328, at 2 ("[A] ccTLD simply is not 'property' subject to attachment."); *id.* at 20 (quoting RFC 1591 for the proposition that "[c]oncerns about 'rights' and 'ownership' of domains are inappropriate").

ICANN would risk a public backlash if it ever claimed to own all domain names. ICANN's role as the IANA, the global coordinator of the DNS, depends entirely on the trust and consent of the global Internet community, a role that could be revoked if the global Internet community were to become dissatisfied.[335] If ICANN were to claim ownership of all domain names, such a move could provoke the Internet community—in particular, foreign nations already leery of management by a U.S. corporation, holders of valuable domain names, and professional domainers—and reignite discussions about replacing ICANN. But just as the prospect of redelegation cuts against ownership of domain names by registry operators, the possibility that ICANN could be removed from its position as global coordinator of the DNS strongly suggests that title to registered domain names does not lie with ICANN.

Second, and related to the first point, ICANN did not officially assume the IANA role until 2000, approximately fifteen years after the DNS became operational.[336] For ICANN to own all domain names, it would need to have acquired those assets from their previous owners, whether registrants or a preceding administrator. However, none of the documents governing ICANN's assumption of the IANA role memorialize any such conveyance.[337] In short, the idea that ICANN ultimately holds title to all registered domain names finds no support in either DNS governance documents or the manner in which ICANN operates.[338]

If registrants do not own their domain names and no DNS intermediary can lay claim to title, then the only remaining possibility is to argue that the global Internet community (GIC) collectively owns all domain names. On its face, this argument seems plausible. Because the GIC could band together to strip ICANN of the IANA function, it could be said that the GIC is the ultimate residuary interest holder. Moreover, the GIC could theoretically establish new policies, whether through its

335. *See* Weinstein v. Islamic Republic of Iran, 831 F. Supp. 3d 470, 488 (D.C. Cir. 2016).

336. *See* IANA Functions Contract between the NTIA and ICANN, §§ 3, 12.2-12.3 (Feb. 9, 2000), https://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf [https://perma.cc/49ZP-YAUF] (formally vesting ICANN with sole responsibility for performing the IANA functions).

337. *See id.* § 4(b); *USC/ICANN Transition Agreement*, ICANN, §§ 2.1, 2.3 (May 14, 2000), https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en [https://perma.cc/4KHC-QWBX] (expressly limiting the assets conveyed by the University of Southern California to ICANN, in transitioning the IANA function to the latter, to certain service marks and logos).

338. Note also that most country code top-level domain delegations predate the formation of ICANN. *See* NAT'L RESEARCH COUNCIL, *supra* note 22, at 126. If ICANN lacks contractual privity with such registry operators, as it does for most ccTLDs, then ICANN would also lack any document evidencing transfer of ownership of domain names in such ccTLDs.

stakeholder position in ICANN or through a successor organization,[339] that cause all domain name registrations to permanently revert back to the GIC upon expiration of their current terms or reallocate domain names in other ways, which individual registrants would be powerless to prevent.

But this proves too much. It is true only in the sense that the citizens of a democratic country, as a collective, "own" all the land in the country. Legal property ownership is a creation of the state,[340] the state itself being a creation of the people in a given territory. The people are thus free, through the apparatus of government, to rewrite the laws of the state to reclaim or reallocate private property. But just because the people of a state could rewrite existing property laws, we would not therefore say that ownership of every estate lies with the general population instead of the individual. Although a sovereign nation may own all land within its borders, it does not follow that the general population of that nation owns each and every lot and house within the land. It likewise does not make sense to place title to individual domain names with billions of undifferentiated people just because the GIC has the power to set DNS policy either through ICANN or by replacing ICANN.

4. A Thought Experiment

Still, the strongest argument that registrants own their domain names may boil down to a simple thought experiment. Suppose that Verisign, the .COM registry operator, declined to renew the registration for the domain name GOOGLE.COM at the end of its current registration period. Suppose further that Verisign's refusal to renew the name did not stem from Google LLC's breach of any registration agreement or other restrictions imposed by Verisign. Instead, exercising its right under the .COM registry agreement with ICANN to reserve any strings in the top-level domain,[341] Verisign simply elected to discontinue registration of the GOOGLE string by any party going forward.

---

339. *See Beginner's Guide to Participating in ICANN,* ICANN at 2, https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf [https://perma.cc/6VJ2-XAK7] (last visited Oct. 18, 2020) (illustrating how members of the GIC could obtain a majority of board seats to guide ICANN policy).

340. JEREMY BENTHAM, THEORY OF LEGISLATION at 111–13 (1931) (C.K. Ogden ed., Richard Hildreth trans., Harcourt, Brace & Co. 1931) (1802).

341. *Base Registry Agreement,* ICANN, *supra* note 73, at § 2.6 ("Registry Operator may ... withhold from registration or allocate to Registry Operator .... additional character strings within the TLD at its discretion.").

Nothing in Verisign's terms for .COM domain names guarantees any registrant the right to renew.[342] And if Google merely leases, but does not own, its domain name, then Verisign, as a lessor, may decline to renew any lease agreement upon its expiration.[343] Google would therefore appear to be without a remedy for the loss of its domain name, other than to pressure ICANN to enact new policies, such as a right-to-renew rule. Yet it seems exceedingly unlikely that Verisign would be able to prevail in court under this fact pattern. Verisign's actions would deprive Google of a billion-dollar asset—likely the most valuable domain name in the world—and it seems far more likely that a court would order the asset returned (effectively mandating renewal) and potentially assess damages for conversion of the asset. Although Verisign's financial and reputational interests discourage the registry operator from acting in this manner, our intuition that a court would not countenance such actions—despite the clear freedom of lessors under property law to cease leasing property at their discretion—strongly suggests that registrants are owners, rather than lessees, of their domain names and that courts would be compelled to draw the same conclusion were the right case presented.

Having established that domain names constitute personal property and that registrants hold title to that property, the next section explores how property rights may be used to protect registrants from DNS censorship.

IV. PROPERTIZATION AS A BULWARK AGAINST DNS CENSORSHIP

In the arena of cloud computing, it's been said that data has mass.[344] By which it is meant that data exerts a gravitational pull on other data and possesses inertia.[345] Unused virtual servers, which represent mere potential processing power, can be scaled down or terminated altogether to reduce or eliminate computing costs. But just as stationary matter still carries weight, data incurs

342. *See generally*, *.COM Registry-Registrar Agreement*, ICANN (Dec. 1, 2012), https://www.icann.org/resources/pages/appendix-08-2012-12-07-en [https://perma.cc/35TG-U5MW].

343. *See* Honoré, *Ownership*, *supra* note 293, at 372 (describing the "right to manage"—an incident of ownership—as "the right to decide how and by whom the thing owned shall be used," which would necessarily encompass the right to decline to lease owned property).

344. *See* HUSENI SABOOWALA ET AL., DESIGNING NETWORKS AND SERVICES FOR THE CLOUD: DELIVERING BUSINESS-GRADE CLOUD APPLICATIONS AND SERVICES 52 (Cisco Press 2013).

345. *See* Dave McCrory, *Defying Data Gravity*, DATA GRAVITAS (Apr. 2, 2011), https://datagravitas.com/2011/04/02/defying-data-gravity/ [https://perma.cc/6LPL-ZUHW].

storage costs, even while at rest. Lightweight applications and services can be copied or migrated easily across similarly configured hardware or even across service providers. But just as greater force is needed to displace increased mass, it may require weeks and thousands of dollars to move a single petabyte of data.[346]

In the same manner, property—whether real or personal, tangible or intangible—has mass, in a sense. By themselves, contract rights can easily be created, modified, or destroyed by the stroke of a pen, the occurrence of a condition, or the breach of a covenant. But when contract terms concern property, they cannot operate with the same freedom of motion. Centuries of property law suddenly attach to the object of agreement, imbuing it with the inertial mass of rights and protections that prevents it from being taken from an unwilling party without commensurate force.[347]

This phenomenon is no less true in the arena of DNS censorship. If domain names are mere service rights, then the battle may be fought almost entirely within the four corners of DNS service agreements, which, being contracts of adhesion, can be crafted to provide every advantage to DNS intermediaries. If, however, domain names are property, then registrants enter into registration agreements with independent protections conferred by property law that can act as counterweights to unlimited contractual power. Whether a DNS intermediary can seize a registrant's domain name becomes no longer an exercise merely to identify a contractual basis to do so, but a careful balancing of interests—the intermediary's contractual right to distance itself from objectionable content weighed against the nature and extent of the registrant's property interest.

Having analyzed the property status of domain names and examined the hitherto neglected issue of title to domain name property in Part III, this Part explores how a robust theory of propertization can be used as a bulwark against DNS censorship. I explain, first, how property rights in domain names can be used to stop domain name seizures by DNS intermediaries. I then analyze where property law, by itself, may fall short, and I consider other potential options to shore up these deficiencies.

346. *See* Dave McCrory, *Data Gravity – in the Clouds*, DATA GRAVITAS (Dec. 7, 2010), https://datagravitas.com/2010/12/07/data-gravity-in-the-clouds/ [https://perma.cc/MS72-T36T] ("Data if large enough can be virtually impossible to move.").

347. *See* Richard R.W. Brooks, *The Efficient Performance Hypothesis*, 116 YALE L.J. 568, 575 (2006) ("Property rules protect entitlements by using the state's police powers to prohibit nonconsensual appropriations, whereas liability rules use court-determined monetary compensation to discourage nonconsensual appropriations.").

A. How Property Law Protects Registrants

As explained *supra*, the locus of title to domain name property significantly affects the balance of power between a registrant and any DNS intermediaries.[348] If a registrant does not own a domain name that she registers but merely leases it from her registrar, then the registrar should have the traditional powers of a lessor. Like a lessor of other forms of property, a registrar may include restrictions in the registration agreement (the lease) concerning how the registrant-tenant may use the domain name property. And the registrar may revoke the registrant's right to possess the property (the leasehold) for violating those restrictions. If, however, a registrant owns her domain name, as I have shown, then the registrar occupies a very different position. A registrar who seizes a validly registered domain name is no longer in the position of a lessor protecting its own property from improper use by a registrant-lessee. Instead, the registrar becomes only a party to a contract for registration-related services, and domain name seizure becomes a general self-help remedy for breach of the registration agreement. When viewed in this manner, contract terms permitting registrars to seize domain names become suspect, and the registrar must point to accepted practices in other areas of law to show that such terms should be enforceable.

In particular, the registrar must identify some analog in which *A* may permanently seize property owned by *B* as a self-help remedy for *B*'s breach of contract. Where *A* has no interest in the property, the breach is unrelated to *B*'s payment obligations,[349] and *A* has no duty to sell the property or otherwise account to *B* for the value of the property seized. For ease of reference in the discussion that follows, I will refer to these criteria as (1) Right to Seizure, (2) Self-Help Remedy, (3) Non-Monetary Breach, (4) Absence of Interest, and (5) No Duty to Account. As potential analogs, I examine the rights afforded to parties under repossession, execution, bailment, and liquidated damages.

1. Repossession

Under the law of repossession, a lender may seize property owned by a debtor when the debtor fails to make timely payments on a loan that was used to purchase the property.[350] Importantly, in certain cases such as vehicle repossession, the lender is permitted to seize the debtor's property immediately once the

348. *See supra* Part III.E.

349. Domain name registration fees are typically paid in advance. Therefore, non-payment would not give rise to a termination for breach.

350. U.C.C. § 9-609.

debtor becomes delinquent without the need to first obtain a court order.[351] Repossession therefore shares two criteria with domain name seizure: Right to Seizure and Self-Help Remedy.

However, under repossession, the creditor may seize the debtor's property only in the event of a monetary breach—namely, the debtor's delinquency in repaying the loan. The resulting lien permits the lender to seize only the property that secures the loan and no other property owned by the debtor.[352] Finally, after repossessing the secured property, the lender must sell it and remit any proceeds in excess of the outstanding balance back to the debtor (minus expenses).[353] A lender who repossesses and sells an automobile for $20,000 may not retain the entirety of the proceeds to satisfy a loan balance of only $5,000. Repossession thus requires proportionality between the value of the property seized and the amount of outstanding principal. Accordingly, repossession fails to meet the remaining three criteria listed above—Non-Monetary Breach, Absence of Interest, and No Duty to Account—and thus fails to provide a suitable precedent for the enforceability of domain name seizure.

2. Execution

I use "execution" as an umbrella term to refer to the forced sale of assets under bankruptcy, garnishment, attachment, or similar proceedings in order to satisfy an outstanding debt.[354] Unlike repossession, in these proceedings, the creditor need not have a pre-existing interest in the particular property seized. Thus, execution meets two of the above criteria: Right to Seizure and Absence of Interest.

However, execution proceedings require a court order—issuance of the appropriate writ—before the debtor's property may be seized.[355] Moreover, like repossession, the creditor is not permitted to retain the seized property but must sell it and account to the debtor for any excess proceeds from the sale.[356] Finally, the

---

351. *See id.* ("A secured party may proceed... without judicial process, if it proceeds without breach of the peace.").

352. *Lien*, BLACK'S LAW DICTIONARY (10th ed. 2014).

353. U.C.C. § 9-615(a), (d). *See also* Russell L. Wald, *Secured Party's Failure to Sell Collateral in Commercially Reasonable Manner*, 4 AM. JUR. PROOF OF FACTS 2D 1 ("After such a disposition, the secured party must account to the debtor for any surplus realized on the disposition, and unless otherwise agreed, the debtor is liable for any deficiency.").

354. *See* FED. R. CIV. P. 69 ("A money judgment is enforced by a writ of execution . . . .").

355. *Writ of execution*, BLACK'S LAW DICTIONARY (7th ed. 1999).

356. *See Execution and Judicial Sales—Procedure—Distribution of Proceeds of the Sale*, 1 L. Debtors & Creditors § 6:62 (Nov. 2019); WASH. REV. CODE. § 6.21.110 ("Any remaining proceeds shall be paid to the judgment debtor . . . .").

remedy is applicable only where the debtor is unable or unwilling to pay some amount due; it does not apply to merely alleged damages. Execution therefore fails on three of the above criteria—Self-Help Remedy, Non-Monetary Breach, and No Duty to Account—and likewise does not provide a suitable analog for domain name seizure.

3. Bailment

Under the law of bailment, a storage contract may entitle a warehouseman to sell a customer's property held in a rented storage unit if the customer has fallen into arrears in order to satisfy any outstanding balance.[357] As with repossession, storage providers who sell a customer's property to satisfy amounts owed need not obtain a court order to act; the remedy is self-help in that regard.[358] Moreover, the remedy may be used to compensate bailees for certain non-monetary breaches, such as to repair damage to the bailee's facilities.[359] Therefore, bailment could be said to satisfy three of the above criteria: Seizure, Self-Help Remedy, and Non-Monetary Breach.

But the bailee's right to sell the bailor's property still differs from domain name seizure in at least two respects. First, bailees automatically acquire a lien on any bailed goods.[360] It is to execute on that lien that the storage provider may sell the bailor's goods.[361] Second, the bailee must account to the bailor for the sale and remit any excess proceeds.[362] Bailment, thus, fails to satisfy two of the criteria of domain name seizure: Absence of Interest and No Duty to Account.

Bailment fails to provide a suitable analog for another, important reason. Inherent in bailment is the fact that the bailor's goods are in the physical possession of the bailee. The bailee's right to sell the goods, therefore, functions not only to compensate the bailee for non-payment but also to relieve the bailee of the goods and to reclaim his space for other purposes. By contrast, a registrar

357. *See* R.H. Helmholz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 KAN. L. REV. 90, 120 (1992) ("Bailees are often given the power to sell bailed goods either under state law (typically to enforce a statutory warehouseman's lien) or under the bailment contract itself (to remedy the nonpayment of the bailor's debt for storage or repair).").

358. *See, e.g.*, WASH. REV. CODE. § 19.150.080 (2007) (conditioning a warehouseman's ability to sell a customer's stored property only on certain non-judicial prerequisites).

359. *See* Helmholz, *supra* note 357, at 120.

360. WILLIAM F. ELLIOTT, A TREATISE ON THE LAW OF BAILMENTS AND CARRIERS § 101 (1914) ("The warehouseman has a right to reasonable compensation . . . and has a lien to secure this.").

361. U.C.C. § 7-206(e).

362. *See, e.g.*, WASH. REV. CODE § 19.150.060(1)(e) (2016).

does not possess a registrant's domain name. Instead, possession lies either with the registry operator, who maintains the registry database and the zone file,[363] or, it could be argued, with the registrant herself. This fact makes bailment an even weaker analogy, since the law does not permit a bailee to seize property *outside* of his facilities to satisfy outstanding debts.

4. Liquidated Damages

A liquidated damages clause is used to specify predetermined damages for breach of a contract where the injury to the non-breaching party may be difficult to quantify.[364] To be enforceable, liquidated damages must be reasonable and non-punitive.[365] Liquidated damages do meet some of the above criteria in that they are awarded for breach of contract that may be unrelated to payment obligations, and the party enforcing a liquidated damages clause need not have a pre-existing interest in property belonging to the breaching party—the Non-Monetary Breach and Absence of Interest criteria.

However, liquidated damages diverge from domain name seizure in that they do not entitle the non-breaching party to seize property belonging to the breaching party. The non-breaching party must first bring suit and obtain a judgment and verdict for damages—monetary damages. Thus, liquidated damages do not satisfy the Right to Seizure and Self-Help Remedy elements of domain name seizure.

Not all forms of liquidated damages require the non-breaching party to bring suit, however. Under Section 2-718 of the Uniform Commercial Code, a seller may withhold delivery of goods for which a buyer has already paid to offset an unrelated breach of contract by the buyer.[366] It could also be argued that although the buyer has not yet received the goods, withholding delivery to a party who has equitable title constitutes a form of seizure. UCC § 2-718, therefore, arguably brings in the Right to Seizure and Self-Help Remedy elements. But it does so at the expense of the Non-Monetary Breach element, since it applies only to payment-related breaches. In any event, liquidated damages, whether in the form of UCC § 2-718 or the common law, fail as a suitable analog to domain name seizure because they must reasonably approximate the injury suffered by

363. *See* Globalsantafe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 625 n. 42 (N.D. Ala. 2013) ("[T]o the extent that domain names, when considered as property, have a 'location, the registry's central database is the logical location of such property.").

364. Resnick v. Uccello Immobilien GMBH, Inc., 227 F.3d 1347, 1350 (11th Cir. 2000).

365. *Id.*

366. U.C.C. § 2-718.

the non-breaching party.[367] This proportionality requirement stands in contrast to the No Duty to Account element.

5. Domain Name Seizure as Tortious Conversion

The above comparisons having failed, one struggles to find a good analog to justify using domain name seizure as a catch-all remedy for breach of a registration agreement.[368] This makes sense. As a matter of public policy, private parties should not have unilateral power to seize property belonging to other parties for general breaches of contract where damages are unknown, minor,

---

367. For example, where a seller withholds delivery of the purchased goods, the buyer is entitled to partial restitution if the value of the goods withheld exceeds the amounts owed to the seller. *See id.*

368. One could alternatively attempt to justify domain name seizure under property law (rather than under breach of contract) by classifying domain name registration as a type of defeasible estate. Analogizing a registrar's acceptable use policy to a condition terminating the registrant's possessory interest in the estate, the registrar could be said to have a future interest in the domain name, and the registrar's right to seizure would function as a right of reverter in a fee simple determinable or fee simple subject to condition precedent. While initially plausible, justifying domain name seizure under a theory of defeasible estates suffers from several fatal flaws.

In the first place, for a registrar to reserve a future interest in a domain name upon registration, the registrar would first need to have full title to the domain name (i.e., fee simple absolute) in order to grant the lesser estate (e.g., fee simple determinable) to the registrant. But as shown above, title does not lay with registrars, who provide only clerical services in domain name registration and administration.

Second, even if title could be said to pass from registrars, the language employed by registration agreements does not clearly evidence the creation of a defeasible estate with a valid future interest reserved to the registrar. *See* Express Media v. Express Corp., 3:06-cv-03504-WHA, at 9 (N.D. CA May 10, 2007) ("Even if the [registration] agreement had been properly authenticated, it still does not have the same effect as a deed."). Courts generally frown upon defeasible estates. JOHN G. SPRANKLING, UNDERSTANDING PROPERTY LAW 124 (4th ed. 2017) ("[One] reason for this hostility is judicial abhorrence of forfeiture. The termination of a defeasible estate is often seen as providing a windfall to the future interest holder . . . , while imposing an inequitable loss on the estate owner."). A number of states have even abolished such estates by legislation. Todd T. Erickson, *Forfeiture of a Public School: A Need to Control the Defeasible Fee*, 63 WASH. U. L. Q. 109, 109 n.1 (1985). And courts will not construe a document as creating a defeasible estate absent clear language to that effect. *Id.* at 116. *See* SPRANKLING, *supra*, at 124–25 ("[W]ords of covenant or promise . . . merely create a contract obligation in the grantee, not a defeasible estate. In addition, where ambiguous language could be construed as creating either an absolute or a defeasible estate, courts uniformly follow a constructional preference for an absolute estate.").

Finally, while courts in some jurisdictions may begrudgingly find defeasible estates under the right conditions, it is not clear that the law has even recognized the validity of defeasible estates in personal property. Christina Mulligan, *A Numerus Clausus Principle for Intellectual Property*, 80 TENN. L. REV. 235, 241–42 (2013) ("Tangible personal property is, in practice, subject to substantially fewer and simpler forms than real property. . . . Although references suggest that personal property might be subject to the same possessory forms that apply to estates in land, there are 'few if any cases that address . . . whether . . . exotic interests such as defeasible fees and executory interests can be created in personal property.'" (quoting Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1, 18 (2000))).

or non-existent. A domain name may appraise for millions of dollars and represent the single most important asset for an online company. And yet, if certain registration terms are to be taken at face value, a registrar may seize that domain name if the registrant so much as fails to update her contact information within seven days[369] or publicly disparages the registrar.[370] A mature legal system should not countenance the forfeiture of so valuable an asset for such speculative harms.

Without precedent for domain name seizure, and with strong arguments against it, it seems plain that contact terms allowing registrars to seize domain names should not be enforceable as a matter of public policy. To the extent a registrar reserves the right to seize a registrant's domain name as a self-help remedy for breach, that contractual right should be negated under the doctrine of unconscionability.[371] To the extent a registrar reserves the right to cancel a domain name for any reason or no reason, the entire registration agreement might be unenforceable as an illusory contract.[372]

It follows, then, that a registrar that takes a registrant's domain name against her will without a legally enforceable right to do so would be subject to common law claims for conversion or trespass to chattels. The tort of conversion, which occurs when a person wrongfully deprives another of possession of or title to an object,[373] would certainly describe a registrar's act of canceling a domain name or transferring it to a new registrant without the previous registrant's permission. Such was the cause of action permitted by the court against Network Solutions in *Kremen*, when the registrar transferred the highly valuable SEX.COM to another party in the absence of a valid right to do so.[374] Conversion further extends to interference with an owner's right to control how her

369. *See* DOMAIN NAME REGISTRATION AGREEMENT, NAME.COM, § 4(a)(i), https://www.name.com/policies/registration-agreement [https://perma.cc/7YLX-D7H9] (last visited Oct. 18, 2020).

370. *See Acceptable Use and Anti-Abuse Policy*, *supra* note 149, at § 1.11.

371. "The concept of unconscionability was meant to counteract two generic forms of abuses: the first of which relates to procedural deficiencies in the contract formation process, such as . . . a refusal to bargain over contract terms, today often analyzed in terms of whether the imposed-upon party had meaningful choice about whether and how to enter into the transaction; and the second of which relates to the substantive contract terms themselves and whether those terms are unreasonably favorable to the more powerful party . . . or otherwise contravene the public interest or public policy . . . ." SAMUEL WILLISTON, UNCONSCIONABLE AGREEMENTS, 8 WILLISTON ON CONTRACTS § 18:10 (4th ed. 2019).

372. *Cf.* Zucarov v. Register.com, 304 A.D.2d 176, 179 (N.Y. App. Div. 2003) (reasoning that a registration agreement could be held illusory if the registrant were not given sole control of his domain name).

373. RESTATEMENT (SECOND) OF TORTS § 222.

374. Kremen v. Cohen, 337 F.3d 1024, 1033 (9th Cir. 2003).

property is used, as does trespass to chattels, even if the owner is not dispossessed of the property itself.[375] Given that suspending a domain name renders it unusable by the registrant, such action could also be tortious, even if the registrar allows the registrant to technically retain ownership by leaving the registration record itself undisturbed.

Limiting registrars' power to seize domain names would not leave registrars without a remedy for breach of their registration agreements. Registrars could still pursue damages and could even terminate all registration-related and value-added services, such as webhosting, DNS privacy, or email services.[376] But, importantly, a registrar should not be permitted to act against the domain name itself. This stands to reason. The domain name is not in the registrar's possession; it lies instead with either the registrant or the registry operator. The registrar need not provide any ongoing services for the domain name to remain operational, authoritative DNS resolution being performed by the registry operator. Accordingly, there can be no justification for permitting a registrar to proactively interfere with an already registered and operational domain name in course of terminating a registration agreement.

Property rights also protect registrants from domain name seizure by other DNS intermediaries. Except in the case of certain country code top-level domains, where the registrar and registry operator may be the same entity, registry operators lack contractual privity with registrants.[377] Thus, unless a registry operator is named as a third-party beneficiary in a registration agreement,[378] the registry operator would have no contractual basis to seize a registrant's domain name for violation of its flow-down terms. Under these circumstances, a registry operator that interfered with a registrant-owned domain name would just as surely be subject to claims for conversion or trespass to chattels. However, if the registry operator is named as a third-party

375. *See* RESTATEMENT (SECOND) OF TORTS § 227 ("One who uses a chattel in a manner which is a serious violation of the right of another to control its use is subject to liability to the other for conversion.").

376. By ceasing to provide registration-related services, the registrar would no longer send notices to the registrant when any of the registrant's domain names approach expiration, nor would the registrar provide any renewal services. It would therefore be incumbent on the registrant to keep track of expiration dates and to transfer any domain names to another registrar in order to renew.

377. *See supra*, Part II.A.

378. Registry operators differ as to whether they wish to have third-party beneficiary status in registrars' registration agreements. *Compare* .JOBS Registry-Registrar Agreement, *supra* note 116, at Exhibit D, § (f) ("Registry Operator is an intended third party beneficiary of the Registrar's Registration Agreement, with a right to enforce the terms and provisions contained therein.") *with* .COM Registry-Registrar Agreement, *supra* note 342 (failing to impose any similar requirement).

beneficiary, the analysis is admittedly more complicated, as explained *infra*.[379]

ICANN does not appear to have engaged in domain name seizure yet in its role as IANA. And it would be difficult for ICANN to do so, given that it has no direct control of registry databases or zone files.[380] That said, if ICANN ever tried to interfere with registered domain names—e.g., by ordering registry operators to take action through ICANN's registry agreements—the same analysis would apply. Whatever contractual rights ICANN might reserve for itself through its flow-down terms, property law should restrict ICANN from seizing assets belonging to registrants as a self-help remedy, especially where ICANN does not perform any core DNS services required to keep domain names operational.

B. Where Property Law Falls Short

As should be clear from the above discussion, the property status of domain names, when properly understood, adds significant protection to registrants in the face of DNS censorship. However, just as trademark law, with its nuanced limitations on geography and field of use, maps awkwardly to the concept of globally exclusive domain names,[381] the equally vintaged principles of property law, forged in an age of horse and socage, are an imperfect substitute for a modern DNS governance framework. While the common law claims of conversion and trespass to chattels do much to protect registrants from heavy-handed contractual terms by DNS intermediaries, they also leave gaps. Those gaps include heterogeneous treatment under state law and a registrant's inability to procure a different provider for registry services if a registry operator remains unwilling to service a domain name.

1. Heterogeneous Treatment under State Law

As a threshold matter, for a registrant to successfully repel DNS censorship using these common law claims, he must first establish that domain names are property; that, as intangible

379. *See infra* Part IV.B.3.

380. *But see* Froomkin, *Almost Free*, *supra* note 118, at 211–12 (noting that ICANN can wield significant power over any registry operator through the threat of making any top-level domain invisible by removing it from the root zone file).

381. *See* Bridy, *Notice and Takedown*, *supra* note 15, at 1354–55 (contrasting trademark rights in real space, which are limited to "specific categories of goods and geographies" and potentially allow different businesses to share the same mark, with a domain name, which "can be controlled by only one person"); A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy"—Causes and (Partial) Cures*, 67 BROOK. L. REV. 605, 608 (2002) ("Trademark law is organized around a set of objectives and assumptions that map badly onto the Internet.").

property, they can be the subject of a conversion claim; and that he holds title to that property. If any of these propositions fails, his defense against contractual terms granting DNS intermediaries broad rights to seize domain names based on website content may also fail. And because "property interests are created and defined by state law,"[382] different states may reach different conclusions on these prerequisites.

Although the status of domain names as property is fairly well established,[383] not all states have had occasion to consider the issue. And at least two jurisdictions have sent mixed messages as to where they stand on this foundational question.[384] Even if a state recognizes a registrant's domain name as property, the registrant may nonetheless be barred from bringing a conversion claim if the state adheres to a strict version of the merger rule.[385] While some courts have found creative ways to skirt the merger requirement—such as finding reason to apply another state's law or characterizing domain names as physical property—other courts have not hesitated to use the merger rule to stop domain conversion claims in their tracks.[386] Finally, even if a domain name is classified as property and the state allows conversion claims concerning intangible property, a registrant would likely need to establish that he holds title to the seized domain name in order to override contractual terms permitting DNS intermediaries to seize the domain name. Although several cases have suggested or implicitly found that registrants own or hold title to their domain names, and although property theory strongly suggests that registrants should be regarded as owners of their domain names, no U.S. court has had occasion to rule squarely on this topic. The issue is therefore unsettled in American law, and it is possible that different courts might arrive at different conclusions in the future.

Given the common law nature of these issues, DNS censorship may be subjected to heterogenous treatment under state law. The result is that two different registrants might publish identical content on their websites. And yet, if DNS intermediaries attempt to take down both domain names, one registrant might successfully repel the attempt in court while the other is permanently deprived of his domain, depending on the locus of the registrant, the intermediary, or the forum.

382. Butner v. United States, 440 U.S. 48, 55 (1979).
383. *See supra*, Part III.C.1.
384. *See* materials cited *supra*, note 249.
385. *See supra*, Part III.C.2.
386. *See supra*, Part III.C.2.

2. Registrars

With respect to registrars, common law claims of conversion and trespass to chattels should generally prevent registrars from canceling, suspending, or transferring registrants' domain names as self-help remedies for contract breach. But registrars remain free to refuse new registrations or to decline to renew existing registrations for any reason or no reason. A marginalized registrant in such situations must rely on his ability to find another registrar who will sponsor his domain name or otherwise become a registrar himself.

3. Registry Operators

With respect to registry operators, as noted previously, if a registry operator that is named as a third-party beneficiary in a registration agreement decides to seize a registered domain name, property law, by itself, might not suffice to protect the registrant from DNS censorship. Unlike registrars, which can terminate their relationships with registrants, and cut off all services in the process, without affecting the operation of already-registered domain names, the same cannot be said of registry operators. A registrant's ability to continue to own and use a domain name depends on two core DNS services that must continually be performed by a registry operator. First, to preserve ownership, the registry operator must maintain the registrant's registration record in the registry database for the top-level domain. Second, to use the domain name, the registry operator must continue to resolve DNS requests for the domain name (Steps 4 and 5 in Fig. 1). Failure to perform the former would allow another party to register the domain name, an outcome tantamount to cancelation or transfer. Failure to perform the latter would make the domain name non-operational, functionally equivalent to suspension. Thus, a registry operator cannot exercise its right to terminate services for violation of its flow-down terms without depriving the registrant of his domain name in the process.

Could a registry operator be compelled to continue to maintain a domain name registration record despite having the contractual right to terminate services for violation of its flow-down terms? Perhaps. Under corporate law, a corporation may be required to maintain various shareholder records such as a stock ledger listing every current shareholder or a list of all voting shareholders.[387] Failure to do so could dilute an existing owner's stake in the corporation or deprive him of his shares altogether. And, given the

387. *See, e.g.*, DEL. CODE ANN. tit. 8, § 219 (2017).

long-recognized status of corporate stock as intangible property,[388] such inaction on the part of a corporation would easily give rise to a claim for conversion of the shareholder's personal property. In a sense, requiring a corporation to maintain an accurate shareholder registry is more akin to a prohibition *against* acting—i.e., improperly assigning an owner's shares to another party—than to a requirement to perform ongoing service.

In the same manner, preventing registry operators from deleting existing registration records should be viewed as an extension of the prohibition against conversion rather than the forced provision of services. Thus, a registry operator should have no more right to seize a domain name owned by a registrant as a self-help remedy for contract breach than a registrar would have. That the registry operator must continue to maintain the registration record of the breaching registrant to avoid running afoul of this prohibition should not change the analysis.

But the same cannot be said for the second core DNS service—resolving DNS requests for the domain name. Unlike the duty to maintain an accurate registry database, which could just as easily be viewed as a prohibition *against* recording competing ownership records, resolving DNS requests is unambiguously a proactive service. A registrant's property interest in his domain name notwithstanding, it's not clear whether courts would prevent a registry operator from exercising its right to terminate DNS resolution services for breach of its contract terms—at least under existing law. Although a registrant would still retain title to his domain name if a registry operator ceased to provide DNS resolution services,[389] the domain would effectively be useless.[390] Many professional domainers are happy to maintain domain names only as investment assets without using them to resolve to any meaningful websites, but those assets carry value only because they could be used to generate web traffic (through DNS resolution) at any time. To perpetually refuse to resolve a domain name is to destroy its value entirely.

Even if registry operators could somehow be prevented from terminating for breach and be compelled to provide DNS resolution

388. *See* Robert Pomerance, *The Situs of Stock*, 17 CORNELL L. REV. 43, 46 (1931).

389. Provided the registration record remains in the registry database. *See* .COM REGISTRY-REGISTRAR AGREEMENT, *supra* note 342, at § 1.8 ("A name in a registry database may be a Registered Name even though it does not appear in a TLD zone file (e.g., a registered but inactive name).").

390. *See* Globalsantafe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 621 (N.D. Ala. 2013) (explaining that when a domain name "is removed from the TLD zone file but the information in the Registry Database is otherwise unchanged," the practical effect is that the domain name is rendered "functionally useless").

services for registered domain names,[391] they, like registrars, nonetheless reserve the right to refuse to register a domain name in the first place or to decline to renew an existing registration for any reason or no reason. And, whereas a registrant might easily replace a registrar that refuses to renew an existing registration, an uncooperative registry operator cannot be replaced. A domain name cannot be transferred to a different registry operator any more than a .COM domain name can be transferred to the .NET top-level domain while remaining the same domain name. If a registry operator refuses to renew an existing domain name, the registrant will inevitably lose her domain name once her current registration term expires.

Could a registry operator be compelled, under current law, to service any and all registration requests? Most likely not. Although the law of common carriage, a subset of the law of bailment, requires certain classes of service providers to transport goods or persons without discrimination,[392] U.S. courts historically have been unwilling to classify telecommunication service providers as common carriers under the common law.[393] Registry operators, therefore, are not likely to be subjected to common carriage requirements absent a statutory basis.[394]

---

391. One argument in favor of requiring registry operators to continue to resolve DNS queries for breaching registrants is that because of registry operators' unique role as authoritative resolvers for top-level domains, they must *always* respond to DNS queries about second-level strings within their top-level domains, whether those strings map to active, suspended, or even non-existent domain names (Steps 4 and 5 in Fig. 1). In responding to a DNS query for an active domain name, a registry operator returns the name of an authoritative nameserver for the domain name, as chosen by the registrant. In responding to a DNS query for a suspended name, a registry operator returns the name of a different nameserver, as chosen by the registry operator, to indicate that the name has been suspended. *See, e.g.*, *Registrar Accreditation Agreement - Verification of WHOIS Details*, MDDHOSTING, https://www.mddhosting.com/support/knowledgebase/1021/Registrar-Accreditation-Agreement—Verification-of-WHOIS-Details.html [https://perma.cc/7PXZ-N4U7] (last visited Oct. 18, 2020) ("Domain suspension involves setting the domain's nameservers to ns1/ns2.verification-hold.suspended-domain.com."). In both cases, the registry operator must respond to DNS queries for the domain name. The only difference is the particular text (the nameserver) sent back in the response.

392. *See* JOHN D. LAWSON, THE PRINCIPLES OF THE AMERICAN LAW OF BAILMENTS § 83 (1895).

393. *Id.* at § 317 ("American Courts have refused to hold telegraph companies to the extraordinary responsibility of a common carrier of goods . . . .").

394. Even the FCC's 2015 Open Internet Order, which established network neutrality rules, before it was superseded by the FCC's 2017 Restoring Internet Freedom Order, did not classify DNS resolution services as "telecommunication services" in order to subject DNS intermediaries to common carriage regulation. *See* Protecting and Promoting the Open Internet, GN. Dkt. No. 14-28, Report & Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, ¶ 356 (Mar. 12, 2015) (rejecting the argument that broadband Internet access services should be classified as "information services," which are not subject to common carriage requirements, when provided in

In sum, although existing property law should generally protect registrants from DNS censorship at the hands of registrars or ICANN, it provides imperfect coverage against a registry operator determined to stamp out an offending domain name. While some registry operators may lack the contractual basis to enforce their flow-down terms, others have established the right to terminate DNS resolution services through third-party beneficiary status and, thus, render controversial domain names useless. And whatever claims a registrant might successfully mount against registrars or registry operators under existing property law for interference during a registration term, both DNS intermediaries can decline to renew an existing domain name for breach of a morality clause, with the refusal of a registry operator ultimately proving fatal.

C. *Filling the Gaps*

This section presents three potential options for filling the gaps left by traditional property law. Those options include enacting new federal law to protect domain names in the United States, leveraging ICANN's top-down power to prohibit DNS censorship, and creating a new DNS altogether.

1. Federal Law

"Property and law are born together, and die together. Before laws were made, there was no property; take away laws, and property ceases."[395] This statement, penned by Jeremy Bentham more than 200 years ago, finds meaningful application in the modern DNS. While traditional, common law doctrines of property and conversion protect domain name owners in important ways, their gaps, if aggressively exploited, could effectively kill domain name property altogether, paving the way for DNS intermediaries to become the new arbiters of speech on the public Internet. One obvious solution to prevent this outcome is to enact new federal legislation to protect registrants from DNS censorship.

On the modest side, such legislation could be relatively simple, doing little more than making explicit Congress's already implicit recognition of domain names as property in the ACPA and the PRO-IP Act.[396] By further establishing registrants' title-rights to their domain name property and providing a federal cause of action for conversion thereof, Congress could solve the problem of

conjunction with DNS and caching services, which the Commission recognized as information services).

395. BENTHAM, *supra* note 340, at 111–13.

396. *See supra*, Part III.D.2.

heterogeneous treatment of domain name theft and interference under state common law.

On the more ambitious side, Congress could enshrine a new class of intellectual property in domain names, on par with federally protected patents, trademarks, and copyrights. Going beyond merely establishing property rights in domain names, such legislation could further ensure that the DNS remains available to all by subjecting DNS intermediaries to common carriage requirements.[397] Preventing registry operators from silencing disfavored viewpoints by declining to renew domain names associated with controversial websites would do much to advance the goal of a content-neutral DNS.

While DNS intermediaries might understandably object to any legislation that shifts power over domain names to registrants, such a federal regulatory scheme could also include important protections for DNS intermediaries. Consider that if property rights prevent DNS intermediaries from seizing registrants' title-held domain names for breach of contract, that prohibition would likely extend to domain names associated with infringing or illegal content. As argued *supra*, a lessor who retains title to his property may retake possession from a breaching lessee under the terms of his lease agreement. But if the non-breaching party sold, rather than leased, the subject property, the law should not afford him the right to re-appropriate the property, where he has no security interest in it, as a general, self-help remedy for breach. Whether the breach stemmed from legal, infringing, or illegal conduct should make no difference in terms of property rights. The seller's rights against a party engaging in illegal conduct are limited to terminating services, not seizing property believed to be used to facilitate the crime.

Federal law could give back to DNS intermediaries what pure property law takes away by enumerating circumstances in which intermediaries could suspend, or potentially even cancel, domain names associated with clearly illegal or infringing content.[398] Or, if it would still be inappropriate to entrust private parties with enforcement of matters better left to courts, Congress could chart a middle course by providing immunity to DNS intermediaries for

397. *See* Dorf, *supra* note 14 (proposing that Congress regulate DNS intermediaries as common carriers).

398. *See, e.g.*, CAL. BUS. & PROF. CODE § 17525 (providing immunity under California law to DNS intermediaries who take action against domain names associated with suspected cybersquatting). The law could also recognize the right of DNS intermediaries to take appropriate action in response to non-payment (where registration fees are paid in arrears), fraud, or activities that directly affect the accuracy, stability, or security of the DNS itself.

taking no action against domain names associated with illegal or infringing content until presented with a court order.[399]

Others might object to federal protection of domain names on the grounds that doing so would require the U.S. to effectively regulate ICANN, a role the U.S. relinquished to the international community in 2016. However, targeted laws affecting certain domain name practices in the United States are not inconsistent with allowing ICANN to remain an independent body or with ICANN's exercise of the broader IANA function. Protecting domain name property at the federal level would no more reassert U.S. control over ICANN than the Ninth Circuit's existing recognition of domain name conversion claims allows California to regulate ICANN. In the first place, Congress could explicitly limit the ambit of the law to domain names registered through registrars or registry operators having a presence in the United States. Moreover, protection could be limited to unrestricted generic top-level domains, leaving other countries free to set their own policies for country code top-level domains (even where a registry operator may be located within the U.S.) and leaving industries free to regulate their own restricted and sponsored top-level domains.

Existing federal laws related to domain names—namely, the ACPA and PRO-IP Act—have successfully coexisted with an independent ICANN.[400] And given the special status of the .COM top-level domain on the Internet, the NTIA currently requires Verisign to operate the .COM registry in a content-neutral manner through the Cooperative Agreement pursuant to which Verisign manages the authoritative root zone file.[401] Thus, the U.S. could prevent DNS censorship solely within its borders without disrupting ICANN's right to self-governance through its international multi-stakeholder process.

---

399. *Cf.* Richard Kirkendall, *Inciting Violence vs Freedom of Speech*, NAMECHEAP (Aug. 20, 2017), https://www.namecheap.com/blog/inciting-violence-vs-freedom-speech/ [https://perma.cc/8CWF-AKFV] (calling for guidelines that would require registrars to act in a content-neutral manner in order to protect registrars from public pressure to take down domain names associated with offensive, but legal, websites).

400. Some states also maintain their own anti-cybersquatting laws—*see* UTAH CODE ANN. § 70-3a-309 (Utah); CAL. BUS. & PROF. CODE § 17525 (California); HAW. REV. STAT. § 481B-21 *et seq.* (Hawaii); LA. STAT. ANN. § 51:300.11 *et seq.* (Louisiana)—a practice that has not apparently conflicted with ICANN's ability to operate under its current global multi-stakeholder process.

401. *See* NTIA, SPECIAL AWARD CONDITIONS NCR-92-18742, AMENDMENT THIRTY-FIVE (35) 1 (Oct. 26, 2018), https://www.ntia.doc.gov/files/ntia/publications/amendment_35.pdf [https://perma.cc/APA8-TC8K] ("Verisign will operate the .com registry in a content neutral manner and that Verisign will participate in ICANN processes that promote the development of content neutral policies for the operation of the DNS.").

2. Top-Down ICANN Policy

Absent federal protection of domain names, ICANN could enforce content neutrality though flow-down terms in its registrar accreditation agreement or registry agreements.[402] However, given ICANN's uniquely powerful position over global DNS policy, inviting ICANN to engage in direct policymaking over Internet content could prove a dangerous proposition. Even if ICANN initially exercised such new powers to ensure DNS content neutrality, one can easily imagine a progression of events through which those powers could eventually be turned to the opposite purpose. Succumbing to public pressure, ICANN might see fit to make narrow exceptions, granting registry operators and registrars latitude to formulate their own policies for the most extreme forms of illegal, violent, or hateful speech. Consistent with historical examples of censorship creep, those exceptions would likely expand over time. In the fullness of time, what began as areas of permissive content regulation might evolve into areas of required content regulation, with ICANN's transformation into a global content regulator complete. Thus, enlisting ICANN to protect content neutrality could very well prove fatal to the cause.

A more measured approach might be for ICANN to simply enumerate the criteria under which a registration may be suspended, canceled, or transferred—for example, limiting such actions to fraud, non-payment,[403] and valid court orders. But this approach could theoretically evolve in a similar manner, again leading to the unintended consequence of greater censorship in the DNS ecosystem. Thus, the goal of a content-neutral DNS might best be served by encouraging ICANN to take a hands-off approach to censorship rather than try to proactively prevent it.

3. Alternative DNS

If protection does not come at the hands of either Congress or ICANN, and if DNS censorship continues to expand, then the only remaining option to ensure an open Internet for all viewpoints may be to create an alternative DNS. Nothing inherent in the world-wide web requires clients to use the existing ICANN-administered DNS to translate human-readable strings into IP addresses. Browsers and DNS resolvers could be configured to point to different nameservers and zone files that stand apart from the current DNS hierarchy.

---

402. *See* Kuerbis et al., *supra* note 142, at 12 ("ICANN's RAA could attempt to prevent registrar terms of service from creating an arbitrary ability to take down a domain based on website content.").

403. In the case of chargebacks or other payment problems.

Although alternative DNS systems have been proposed and even attempted in the past,[404] the broader Internet community has not found a sufficiently compelling reason to adopt a competing service. DNS censorship could change that.[405] Moreover, the advent of blockchain-based technology has now made the once-impractical idea of a decentralized DNS a real possibility, as some experts have proposed.[406] Apart from protecting domain names from interference by governments or private parties, shifting the burden of maintaining authoritative zone files and resolving DNS requests to a distributed ledger could obviate the need for registration and renewal fees and yield other interesting benefits.[407]

To be sure, many details would need to be worked out to implement an alternative DNS. And creating a parallel authority could introduce new problems related to naming collisions and trademark rights. But if nothing else, given ICANN's strong desire to avoid a split-root world,[408] the possibility of a competing DNS could alert ICANN and DNS intermediaries to the risk that DNS censorship imposes to their hegemony and spur them to take action. It should therefore be explored in earnest.

CONCLUSION

In the heady, innocent days of the early Internet—when collaborating universities sought only to create an easier way to keep track of each other's host servers—the notion of domain names as property seemed both unnecessary and inappropriate. But with the rampant commercialization of cyberspace in the 1990s and

404. *See generally* NAT'L RESEARCH COUNCIL, *supra* note 22, at 99 (acknowledging the initial success of NET.NET—now defunct—which offered additional top-level domains not delegated by ICANN); Milton L. Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction?*, 3 J. NETWORK INDUS. 313 (2002); Nancy Scola, *When the Internet Nearly Fractured, and How It Could Happen Again*, THE ATLANTIC, (Feb. 24, 2011) https://www.theatlantic.com/technology/archive/2011/02/when-the-internet-nearly-fractured-and-how-it-could-happen-again/71662/ [https://perma.cc/6FXS-N7MF].

405. *See* Froomkin, *Almost Free*, *supra* note 118, at 215 ("[T]here is only so much that most registrants would put up with before walking away from domain names and towards some alternative.").

406. *See* Brendan Benshoof et al., *Distributed Decentralized Domain Name Service*, 2016 IEEE INTERNATIONAL PARALLEL AND DISTRIBUTED PROCESSING SYMPOSIUM WORKSHOPS (proposing a decentralized DNS based on a distributed hash table and the blockchain protocol). PeerName claims to be the first registrar to offer decentralized domain names based on an alternative, blockchain-powered DNS and to have already registered 6,000 domains under unofficial TLDs, such as .BIT, .COIN, and .ETH. *See* PEERNAME, https://peername.com/about [https://perma.cc/E9CL-XLHX] (last visited Oct. 18, 2020).

407. *See supra*, Part III.E.2.

408. *See* Weinstein v. Islamic Republic of Iran, 831 F.3d 470, at 487 (D.C. Cir. 2016) (describing ICANN's interest in preventing another entity from establishing a competitive root zone file).

early 2000s, it became clear that domain names not only possessed immense economic value but also shared enough core similarities with other commercial assets that their status as property could not be denied. Until recently, merely classifying domain names as property sufficed to protect registrants from would-be domain thieves through the classic, property-based torts of conversion and trespass to chattels. But with the rise in private censorship by DNS intermediaries, elucidating the precise nature of that property interest has become essential to determining whether intermediaries may seize domain names based on registrants' controversial, but clearly legal, speech.

Careful analysis of the property nature of domain names and the roles that intermediaries play in the DNS shows that locating title to domain names with registrants is the most defensible conclusion. Once that premise is established, it becomes clear that the law should not permit DNS intermediaries to seize registrants' domain name property as a self-help remedy for contract breach. And, without an enforceable contractual right for intermediaries to do so, registrants could successfully bring claims against interfering intermediaries for conversion or trespass to chattels. Thus, a robust theory of the property nature of domain names goes a long way toward protecting registrants from DNS censorship.

But centuries-old doctrines of property law do not map cleanly to the modern, global DNS, leaving registrants vulnerable to registry operators who refuse to register or renew domain names that violate their self-constructed moral standards. Congress or ICANN could shore up these deficiencies by passing laws (in the case of Congress) or establishing contractual policies (in the case of ICANN) that protect domain names associated with legal websites from seizure and potentially even establish a public right to register and renew domain names without discrimination based on viewpoint. If either body fails to act and content regulation continues to grow unabated, minority resistance to DNS censorship could eventually rise to the level of creating competing, decentralized systems for name-to-address translation.

Short of these supplements, however, existing property law can still do much to protect registrants from DNS censorship at the hands of registrars or even of ICANN. The crucial question, therefore, becomes whether courts will themselves practice the neutrality required to treat laudable and execrable registrants alike. It's been said that hard cases make bad law. If a trillion-dollar, upstanding corporation could prevail on a conversion claim for the loss of GOOGLE.COM despite clear contractual terms justifying seizure or non-renewal—a case that is unlikely ever to arise—the operators of offensive and hateful sites like

DAILYSTORMER.COM should prevail on similar facts—cases that will inevitably find their way to courts over the next several years.[409]

[409] As this article was going to press, public outrage over the January 6, 2021 storming of the United States Capitol Building resulted in heightened attention to the role of online platforms in disseminating disinformation, hosting extremist content, and serving as points of coordination for potentially violent activity, with the result that various individuals, groups, and websites were suspended or permanently banned by certain online service providers. *See* Editorial Board, *The Progressive Purge Begins*, WALL STREET J. (Jan. 10, 2021), https://www.wsj.com/articles/the-progressive-purge-begins-11610319376 [https://perma.cc/4W84-9QB3]. While most of these takedown actions appear to be confined to higher levels of the Internet stack—a topic on which this article expresses no opinion—the broader the movement to stem the flow of controversial content managed to find its way down to the DNS in certain cases. For example, on January 11, 2021, registrar GoDaddy suspended the domain name AR15.COM, associated with the largest online gun forum, over user content that "promotes and encourages violence." Andrew Allemann, *GoDaddy explains AR15 .com boot*, DOMAIN NAME WIRE (Jan. 17, 2021), https://domainnamewire.com/2021/01/17/godaddy-explains-ar15-com-boot/[https://perma.cc/5CUC-G39H]. In response, the website operator transferred the domain name to Epik.com, a registrar that markets itself as free-speech friendly. *Id.*; *supra* note 206. Perhaps fearing similar treatment by its registrar, Parler, the right-leaning Twitter-alternative, preemptively transferred its domain name to Epik after numerous service providers cut ties to the social network following the Capitol riot. *See* Danya Hajjaji, *What Is Epik? Parler Domain Finds New Home In Far Right's Preferred Hosting Service*, NEWSWEEK (Jan. 12, 2021), https://www.newsweek.com/parler-domain-new-host-service-epik-1560880 [https://perma.cc/U8X4-GPG7]. As described *supra* in Part II.C, the risk that DNS censorship poses to free expression on the Internet depends on whether alternative avenues for maintaining domain names associated with controversial websites continue to exist and, thus, on which entities in the DNS governance hierarchy play a role in enforcing content restrictions. One potential bellwether of a move toward greater top-down enforcement of DNS-based content restrictions may be the fate of content-neutral registrars like Epik. Thus, it will be of particular interest to Internet governance scholars whether the coming years see coordinated efforts to pressure registry operators and ICANN to exert more control over such registrars and their content policies (e.g., by threatening de-accreditation or denying access to registration systems) and how registry operators and ICANN respond to that pressure.