

INTERNET INFRASTRUCTURE AND CONTENT MODERATION IN THE SHADOWS

JELENA LAKETIĆ*

While the current scholarly debate on content moderation primarily focuses on the activities of online platforms, it is crucial to recognize the equally important, yet mostly overlooked, infrastructure-level moderation. Internet infrastructure actors, such as the Domain Name System (DNS), play a crucial role in the functioning of the internet and are increasingly receiving demands to moderate user content. Notably, DNS management is overseen by the Internet Corporation for Assigned Names and Numbers (ICANN), which makes it an attractive target for content monitoring by governments and censorship advocates.

Governmental pressures on ICANN to moderate content exist internally through policy influence within the multistakeholder community and externally through recent EU Regulation. This Article argues that the ICANN should steadfastly focus on the stability of the technical infrastructure and refrain from content moderation. The potential consequences of not adhering to this posture are grave. Without this focus, the DNS could become a powerful tool for suppressing the speech of internet users, including political dissent and minority views.

Even though ICANN sits atop the DNS governance hierarchy, its multistakeholder bureaucracy is complex and intricate. Importantly, governmental representatives, such as the Governmental Advisory Committee (GAC), often initiate policy parameters within ICANN. This Article explains how ICANN, as the

*University of California, Berkeley, School of Law, Doctoral Candidate (J.S.D). Lloyd M. Robbins Fellow. Many thanks to Professor Manisha Padi for her support and the editors of the Colorado Technology Law Journal for their insightful suggestions and professionalism.

overseer of DNS management, suffers from internal pressures to moderate content through its sophisticated contractual framework.

Moreover, this Article emphasizes that a thorough examination reveals that the EU Digital Services Act (DSA) shifts content moderation practices toward internet infrastructure, including the DNS. This aspect of the DSA, entirely overlooked in existing scholarly literature, has the potential to fundamentally alter how online content is regulated and monitored. The urgency of this shift demands immediate attention.

INTRODUCTION

Current debates on content moderation primarily focus on the role of online platforms such as Facebook or YouTube.¹ Online platforms are in the spotlight because they can “screen, rank, filter, and block user-generated content”² on a massive scale.³ While the current discourse on content moderation is predominantly centered on the activities of online platforms, it is crucial to recognize the equally important, yet often overlooked, role of infrastructure-level moderation. This less visible form of moderation operates within the layers of “basic internet services,”⁴ including internet domain name registries and registrars. These entities, integral to the Domain Name System (DNS), ensure the smooth routing of online traffic by providing digital addresses and ways of finding them.⁵ In

1. See generally James Grimmelman, *The Virtues of Moderation*, 17 YALE J.L. & TECH. 42 (2015); Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

2. See Hannah Bloch-Wehba, *Automation in Moderation*, 53 CORNELL INT’L L.J. 41, 42 (2020) (“[C]ontent moderation’—the set of practices that online platforms use to screen, rank, filter, and block user-generated content.”).

3. See, e.g., Maddy Osman, *Wild and Interesting Facebook Statistics and Facts*, KINSTA (July 19, 2024), <https://kinsta.com/blog/facebook-statistics/> [<https://perma.cc/XY5M-4AZD>] (noting how in just one minute “510,000 comments are posted, 293,000 statuses are updated, 4 million posts are liked, and 136,000 photos are uploaded” on Facebook).

4. See Jack Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011, 2038 (2018) (“[B]asic internet services [include] . . . [d]omain name services, which include registrars that register domain names (such as GoDaddy), registries that run top-level domains (such as Verisign), and DNS providers that resolve domain names (such as Cloudflare and Google).”).

5. See Marshall Brain et al., *How Domain Name Servers (DNS) Work*, HOWSTUFFWORKS (Mar. 7, 2024), <https://computer.howstuffworks.com/dns.html> [<https://perma.cc/TME9-PJH7>] (explaining DNS functions).

2020, the relevance of DNS was recognized by the EU's Cybersecurity Strategy for the Digital Decade.⁶

Since the recognition of DNS's role in content moderation, the concept of "meta-moderation or second-order moderation"⁷ is gaining more scholarly attention.⁸ This shift in focus on who should moderate content prompts us to consider questions such as whether domain name registrars should do more to remove online hate speech⁹ or misogyny,¹⁰ or whether they should stay out of moderating content entirely. In other words, should domain name registrars police website content or maintain a strict focus on the stability of the technical infrastructure so that users' web page queries and emails are routed to the precise servers? This is the question at the heart of the infrastructure content moderation debate, a debate that will significantly impact content moderation research in the following years.

Some legal scholars view this question as a "rapidly evolving part of the content moderation ecosystem,"¹¹ while others are more skeptical. For instance, Jack Balkin, a constitutional law professor at Yale Law School and the founder and director of Yale's Information Society Project—a center focused on studying law and new information technologies—has argued that basic internet services should not engage in content moderation.¹² Balkin also

6. See *The EU's Cybersecurity Strategy for the Digital Decade*, EUROPEAN COMMISSION (Dec. 16, 2020), <https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-strategy-digital-decade-0> [<https://perma.cc/KZF7-AFLF>].

7. Christoph Busch, *Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation*, 27 UCLA J.L. & TECH. 32, 37 (2022).

8. See JENNA RUDDOCK & JUSTIN SHERMAN, WIDENING THE LENS ON CONTENT MODERATION, at i (Am. U. Wash. Coll. L. 69th ed., 2021) ("But Facebook is not the internet, and focusing almost exclusively on the companies behind these high-profile social media platforms means that the majority of the internet is often left out of the conversation about how to effectively combat harmful content online while also protecting fundamental rights and civil liberties."); See generally Annemarie Bridy, *Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation*, 74 WASH. & LEE L. REV. 1345 (2017); Nicholas Nugent, *Masters of Their Own Domains: Property Rights as a Bulwark Against DNS Censorship*, 19 COLO. TECH. L.J. 43 (2021).

9. Catherine Shu, *Far-right Social Network Gab Goes Offline After GoDaddy Tells it to Find Another Domain Registrar*, TECHCRUNCH (Oct. 28, 2018, 10:28 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/8A5R-HQK9>].

10. 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/8XHR-BK4F>].

11. Busch, *supra* note 7.

12. Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media*, 1 J. FREE SPEECH L. 71, 73 (2021) ("For basic internet services the regulatory answer is pretty simple: non-discrimination. Let the bits flow freely and efficiently. Don't engage in content regulation at this level.").

warned us that “new school speech regulation” will be directed at infrastructure, not the speakers.¹³ Similarly, Laura DeNardis, Endowed Chair in Technology, Ethics, and Society at Georgetown University, years ago warned about the potential misuse of DNS and its cooption for purposes utterly unrelated to its initially constructed technical functions.¹⁴

This Article asserts that the warnings from Balkin and DeNardis are well-founded and align in the realm of infrastructure-level content moderation. In elucidating this alignment, this Article makes two significant contributions. First, it provides a comprehensive examination of the DNS ecosystem. Second, it delineates two distinct ways in which government actors seek to coopt DNS architecture for content moderation, both through policy influence within the multistakeholder community and through regulation.

As Balkin noted, “the regulation and surveillance of speech require an infrastructure.”¹⁵ What infrastructure is better than the one with “the power of virtual life and death”¹⁶ like the DNS?

It is said that the “DNS defines a central authority for the [i]nternet.”¹⁷ To understand the value of the DNS, we should first know that the internet is a global collection of interconnected computer networks that allows communication using unique numerical Internet Protocol (IP) addresses.¹⁸ Because those IP addresses are hard to memorize, human-friendly domain names were invented.¹⁹ DNS “provides a way of associating alphanumeric names, which are easier for humans to use, with the numerical addresses that designate every location on the [i]nternet.”²⁰ For

13. See Balkin, *supra* note 4, at 2015 (explaining how new school speech regulation is directed at infrastructure and not the speakers).

14. Laura DeNardis, *Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance*, 15 INFO. COMM. & SOC'Y 720, 720-38 (2012).

15. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2297 (2014).

16. Hans Klein, *ICANN and Internet Governance: Leveraging Technical Coordination To Realize Global Public Policy*, 18 INFO. SOC'Y 193, 197 (2002) (describing internet naming space).

17. *Id.* at 196.

18. See *Off. Depot, Inc. v. Zuccarini*, 596 F.3d 696, 698 (9th Cir. 2010) (“Every computer connected to the Internet has a unique Internet Protocol (‘IP’) address.”).

19. See *Acad. of Motion Picture Arts & Scis. v. Network Sols. Inc.*, 989 F. Supp. 1276, 1281 n.1 (C.D. Cal. 1997) (“An IP number is four groups of digits separated by decimal points, for example, ‘013.917.114.41.’ These IP numbers are converted into a more user-friendly, letter-based format called a ‘domain name’ by specialized computers called ‘domain name servers.’”); See also *Office Depot, Inc.*, 596 F.3d at 698 (“Every computer connected to the Internet has a unique Internet Protocol (‘IP’) address.”).

20. NAT'L RSCH. COUNCIL, SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION, NATIONAL ACADEMIC PRESS, vii (2005).

example, DNS translates a more familiar `www.google.com` into a hard-to-memorize IP address, `173.194.33.174`. In this translation process, DNS creates a chokepoint that can be used to control what is and is not accessible online based on its hierarchical design.²¹ As such, DNS provides a channel to sanction internet users and can serve as an essential resource in controlling online content. Denial of access to domain names is equivalent to expulsion from the internet. Merely registering a domain name is not enough to make it truly functional. When a user enters a domain name, a DNS query is sent to the registry operator for the corresponding IP address. Without proper DNS resolution, the domain is useless.²²

Notably, DNS governance and administration are overseen by a California-based non-profit organization, the Internet Corporation for Assigned Names and Numbers (ICANN).²³ This makes ICANN an attractive focus for those who want more content monitoring on the internet.

This Article seeks to enrich the ongoing discourse through two significant contributions. First, this Article introduces the latest European developments to the ongoing debate. The EU's Digital Services Act (DSA)²⁴ stands as a pioneering example of "new-school speech regulation," and is striving to leverage privately owned internet infrastructure for its regulatory purposes. While the DSA primarily focuses on online platforms, it has been argued that it could become the world's most significant attempt to moderate online content.²⁵ However, its effects on moderation at the level of internet infrastructure are frequently overlooked. This Article seeks to explore that dimension.

It argues that a more thorough examination reveals that the DSA tries to coopt DNS and expand content moderation practices to include internet infrastructure. The potential impact of the

21. See Stefan Bechtold, *Governance in Namespaces*, 36 LOY. L.A.L. REV. 1239, 1267 (2003) (noting that the DNS is not a monolithic system, but organized network of databases organized hierarchically).

22. Klein, *supra* note 16, at 195 ("In a manner of speaking, the name space is the Internet. In order to exist on the Internet, a computer must be listed in the name space. Without a listing (without a domain name and an IP number) a computer cannot be found by others. Removal of a computer's listing from the name space constitutes a kind of banishment, for a computer disappears from the list of addressable computers. Whatever entity controls the name space database effectively controls the Internet.").

23. ICANN, <https://www.icann.org/en/beginners> [<https://perma.cc/FH3T-LF7E>] (last visited Feb. 9, 2025).

24. Council Regulation 2022/2065, 2002, O.J. (L 277) 1 [hereinafter DSA].

25. See generally Dawn Carla Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, 24 CHI. J. INT'L L. 115 (2023); See also Anupam Chander, *When the Digital Services Act Goes Global*, 38 BERKELEY TECH. L.J. 1067, 1072-74 (2023) (explaining how a number of mechanisms might globalize the DSA).

DSA's cooption of DNS is not to be underestimated, as it could lead to a fundamental shift in how internet online content is regulated and monitored. While the DSA is shifting the narrative towards basic internet infrastructure, unknowns remain regarding the DSA's applicability to DNS services. The DSA does not provide clear classifications regarding which "intermediary services" categories may apply to various DNS services. This ambiguity raises important questions about effectively maintaining and providing essential DNS services while ensuring legal certainty. Moreover, protecting and enhancing freedom of information and expression and other fundamental rights is crucial. These issues become increasingly urgent as some DNS registrars also provide separate hosting services. It remains unclear whether they fall under the scope of the DSA. Addressing these questions is essential for navigating the evolving landscape of digital services and maintaining the integrity of our online freedoms.

History shows that the US-based ICANN has previously made drastic changes to avoid considerable fines from an EU legislative act. For example, ICANN has restricted the amount and type of data about internet domain name holders to ensure adequate legal compliance with the EU General Data Protection Regulation (GDPR).²⁶ With the introduction of the EU's DSA, we may soon witness ICANN making more transformative changes to adapt to the evolving regulatory landscape.

Second, this Article addresses policy efforts within ICANN related to content moderation. ICANN's position has been described as ambivalent but hesitant to moderate content generally.²⁷ However, these descriptions omit the significant impact of government efforts to achieve content moderation through influencing policy within the multistakeholder community. Even though ICANN sits atop the DNS governance hierarchy, its multistakeholder bureaucracy is complex and intricate, and

26. See Tara M. Aaron, *Availability of WHOIS Information After the GDPR—Is it Time to Panic?*, 108 TRADEMARK REP. 1129, 1133 (2018) (describing the effects of the GDPR on WHOIS database for checking domain name availability or to discover the contact information of a domain name holders).

27. See Sebastian Felix Schwemer et al., *Liability Exemptions of Non-Hosting Intermediaries: Sideshow in the Digital Services Act?*, 8 OSLO L. REV. 4, 15 (2021). See also Aaron, *supra* note 26, at 1336-40 (noting that although ICANN resisted direct involvement in content moderation activities, it accommodated right holders by altering its contracts with DNS intermediaries to support a system of domain name cancellation about which right holders complained).

governmental representatives are often involved with its policy.²⁸ This Article explains how ICANN has suffered from internal pressures to moderate content through its sophisticated contractual framework.

More recently, in June 2024, the ICANN Board decided that its bylaws do not allow it to enforce any contractual commitments that involve content regulation.²⁹ This Article argues that ICANN's decision is correct. Since ICANN holds a prominent position in the global DNS, placing ICANN at the center of online content moderation policymaking could be dangerous for free speech online.

This Article is organized into three major Parts. Part I explains how the EU is shifting the narrative around core infrastructural intermediaries within the DSA framework. Part II provides an overview of the DNS ecosystem and its relevant components, whose nature was not clarified by the European legislator. Part III explains the demands within ICANN to moderate content and how ICANN has freed itself from them. Moreover, it clarifies why internet infrastructure represents a gray zone within the DSA, in addition to raising serious questions about the effectiveness of remedies by DNS intermediaries. In other words, this Part explains why shifting content moderation towards internet infrastructure would set a dangerous precedent. Finally, this Article concludes that whereas the internet's infrastructure layer might be appealing for content moderation purposes, DNS should steadfastly focus on the stability of the technical infrastructure and refrain from content moderation.

I. DSA AND INFRASTRUCTURE LAYER OF THE INTERNET

The EU legal framework regulating online intermediaries has undergone significant changes in recent years. In a departure from previous content moderation initiatives, which focused on specific types of content,³⁰ the DSA takes a broad, horizontal approach

28. See generally OLGA CAVALLI & JAN AART SCHOLTE, *The Role of States in Internet Governance at ICANN*, in POWER AND AUTHORITY IN INTERNET GOVERNANCE: RETURN OF THE STATE? 37 (Blayne Haggart et al. eds., 2021) (examining the role of the state in governance of global internet infrastructure at the ICANN, with particular attention for the Government Advisory Committee).

29. See *Approved Resolutions | Regular Meeting of the ICANN Board | 8 June 2024*, ICANN, (June 11, 2024), <https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-regular-meeting-of-the-icann-board-08-06-2024-en> [<https://perma.cc/6MEB-GMCH>].

30. See, e.g., Directive 2019/790, of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market, 2019 O.J. (L 130) 92 (focusing on copyright content); Regulation 2021/784, of the European

encompassing a wide spectrum of online intermediaries.³¹ The geographic reach of the DSA is extensive,³² and it defines content broadly,³³ including “lawful but awful” content, which refers to content that is not illegal but is considered harmful or offensive.³⁴ Intermediary services can delete content or user accounts or disable access to it when moderating content.³⁵

In addition, many provisions of the DSA are vague.³⁶ The DSA refrains from drawing a clear line between legal and illegal content. Instead, it defines several liability exemptions, illustrating when an online intermediary service provider cannot be held liable regarding third-party content. Those liability exemptions are based

Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online, 2021 O.J. (L 172) 79 (focusing on terrorist content); Directive 2018/1808, of the European Parliament and of the Council of 14 Nov. 2018 Amending Directive 2010/13, on the Coordination of Certain Provisions Laid Down by Law, Regulation, or Administrative Action of Member States Concerning the Provision of Audiovisual Media Services, 2018 O.J. (L 303) 69 (focusing on audiovisual content).

31. DSA, *supra* note 24, at art. 3(g) (defining a “intermediary service” as one of the following information society services: “(i) a ‘mere conduit’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; (ii) a ‘caching’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients upon their request; (iii) a ‘hosting’ service, consisting of the storage of information provided by, and at the request of, a recipient of the service.”).

32. DSA, *supra* note 24, at art. 2(1) (“This Regulation shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment.”).

33. DSA, *supra* note 24, art. 3(t) (“[C]ontent moderation’ means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetization, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient’s account.”).

34. Martin Senftleben et al., *How the European Union Outsources the Task of Human Rights Protection to Platforms and Users: The Case of User-Generated Content Monetization*, 38 BERKELEY TECH. L.J. 933, 976-77 (2023); See also Daphne Keller, *Lawful but Awful? Control Over Legal Speech by Platforms, Governments, and Internet Users*, U. CHI. L. REV. BLOG (June 28, 2022), (explaining “lawful but awful” content in more detail).

35. DSA, *supra* note 24, at art. 3(t).

36. Martin Husovec, *Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules*, 38 BERKELEY TECH. L.J. 884, 901 (2023) (noting that the DSA is the “mix of very specific procedural rules and vague aspirational regulatory expectations” and that “many expectations are purposely vague.”).

on an intermediary's functions as merely transmitting,³⁷ caching,³⁸ and hosting.³⁹ This is an important aspect regarding content because the DSA has a tiered system of obligations: in addition to the general obligations that apply to all intermediary services, additional obligations are assigned to specific categories of intermediary services. For example, while all providers of intermediary services from outside the EU must designate a legal representative in one of the EU Member States,⁴⁰ only hosting services are required to put mechanisms in place to allow any individual or entity to notify them of the presence of information considered to be illegal on their services.⁴¹

The DSA's inclusion of internet infrastructure within its scope is another significant departure from earlier initiatives.

37. DSA, *supra* note 24, at art. 4(1) ("Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the service provider shall not be liable for the information transmitted or accessed, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.").

38. DSA, *supra* note 24, at art. 5(1) ("Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient or more secure the information's onward transmission to other recipients of the service upon their request, on condition that the provider: (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and (e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a judicial or an administrative authority has ordered such removal or disablement.").

39. DSA, *supra* note 24, at art. 6(1) ("Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.").

40. DSA, *supra* note 24, at art. 13(1) ("Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person to act as their legal representative in one of the Member States where the provider offers its services.").

41. DSA, *supra* note 24, at art. 16(1) ("Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means.").

Nevertheless, the devil is in the details. Those seeking evidence of sweeping shifts in the newly adopted EU approach will not find proof in any of the articles. But the evidence is in the recitals, and this does not necessarily diminish its significance. It is worth noting that the European Court of Justice often uses recitals to resolve ambiguity in related legislative provisions.⁴²

The DSA's recitals acknowledge the growing complexity of the online ecosystem, noting that "new technologies have emerged that improve the availability, efficiency, speed, reliability, capacity and security" of internet services.⁴³ Such services establish and facilitate the proper functioning of the internet, including "domain name system (DNS) services, top-level domain name registries, [and] registrars."⁴⁴ This inclusion of the DNS marks a significant change, particularly when compared to recent EU regulations on content moderation that explicitly exclude "providers of domain name systems (DNS)" from their scope of application.⁴⁵ The impact of this policy shift is profound, underscoring the importance of these changes.

Notably, the DSA only mentions internet infrastructure services in the context of benefiting from the liability exemption rules. "[S]ervices establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions,"⁴⁶ can benefit from the liability exemption rules "to the extent they constitute a mere 'conduit,' 'caching' or 'hosting' service," which should be assessed on a case-by-case basis.⁴⁷

Although this approach seems simplistic, there still appears to be a large area of legal uncertainty. This approach does not account for the DNS's technical conditions, nor does it define the DNS and its components. Before considering the DSA's negative impact on the DNS ecosystem in Part III, Part II will highlight the DNS's actual functions.

42. See e.g., *P. Moskof AE v. Ethnikos Organismos Kapnou*, Case C-244/95, 1997 E.C.R. I-6445 (responding to a question about whether a provision was transitory).

43. DSA, *supra* note 24, at recital 28.

44. See Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online [hereinafter TERREG].

45. *Id.*

46. DSA, *supra* note 24, at recital 28.

47. DSA, *supra* note 24, at recital 29.

II. FUNCTIONS OF THE DNS

DNS is a hierarchical system that plays a vital role in the internet ecosystem. It translates unique numerical IP addresses into unique alphabetical domain names, simplifying the process for end users to remember and enter these names into their connected devices.⁴⁸ Put differently, DNS facilitates the exchange of online content. It is also a critical component in email and online communication.⁴⁹ Any website, email, or internet communication on any device that connects to the web—from computers and phones to gaming systems and cars—typically relies on a domain name.⁵⁰

Three key observations shed light on the DNS architecture. First, the DNS ecosystem is hierarchical. ICANN ensures the effective and coordinated management of this system. This makes ICANN a prime target for content monitoring by governments and censorship advocates.⁵¹ Second, while DNS is a key facilitator of online communication and content exchange, it does not directly handle the flow of content.⁵² Third, ICANN is almost exclusively a private entity.⁵³

These observations are crucial in understanding DNS control over online activities. Because the DSA encompasses a large ecosystem of different actors that maintain the technical infrastructure, intermediaries’ roles in addressing content moderation obligations depend on both the type of content and the

48. See *Office Depot, Inc.*, 596 F.3d at 698.

49. See e.g., Jennifer Mingus, *E-mail: A Constitutional (and Economical) Method of Transmitting Class Action Notice*, 47 CLEV. ST. L. REV. 87, 97 (1999) (“The domain, like a street address, tells the e-mail provider exactly which computer to deliver an e-mail message to.”).

50. See e.g., *How DNS and Email Work Together*, CONSTELIX DNS (Nov. 15, 2021), <https://dnsmadeeasy.com/resources/the-interplay-between-dns-and-email-an-essential-guide-for-dns-professionals> [<https://perma.cc/X9PR-SNZA>]

51. 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 [using the DNS] could recreate the kind of control they once had over traditional territorial media.”); See also Allen R. Grogan, *ICANN is Not the Internet Content Police*, ICANN (June 12, 2015), <https://www.icann.org/en/blogs/details/icann-is-not-the-internet-content-police-12-6-2015-en> [<https://perma.cc/BLAS-SXQZ>] (explaining how some members of the internet community advocated that ICANN should assume greater responsibility for policing online content).

52. See Nugent, *supra* note 8, at 55 (noting that “no content ever flows through the DNS itself, whether website, email, video, chat, or other content.”).

53. See e.g., Tobias Mahler, *Generic top-level domains: A study of transnational private regulation 16-39* (2019) (explaining the diminishing influence of the US government over the DNS and ICANN’s evolution to a global private regulatory regime outside traditional categories of domestic or international law).

technical services they provide. Therefore, understanding what DNS does and does not do becomes fundamental.

A. *Technical overview of the DNS Hierarchical Functions*

Understanding a domain name and its components is crucial for comprehending the DNS. Most domain names consist of three parts, each separated by a period, such as “http://www.google.com.”⁵⁴ The hierarchy levels of a domain name are read from right to left.⁵⁵ Therefore, the first segment of a domain is the Top-Level Domain (TLD) (http://www.google.com), while the second part (http://www.google.com) is a Second-Level Domain (SLD).⁵⁶

Additionally, DNS intermediaries, with their technical expertise, play a pivotal role in enabling internet communications. They are responsible for registering,⁵⁷ renewing,⁵⁸ and resolving domain names,⁵⁹ functions crucial for the smooth operation of the internet.

DNS is a multi-step process that begins with domain name registration. Registries and registrars are necessary for domain name registrations, and they have different but complementary tasks.

A domain name registry is an authoritative master database of the TLDs.⁶⁰ It typically has a technical role and “keep[s] the master database of all domain names registered in each top-level domain (TLD) and generate[s] the ‘zone file’ that allows computers to route internet traffic to and from TLDs anywhere in the world.”⁶¹

54. *Office Depot, Inc.*, 596 F.3d at 698 (“The hierarchy of each domain name is divided by periods.”).

55. *Id.*

56. The acronym “www” compacts the initials of the “World Wide Web” and the acronym “http” means a transmission protocol based on “Hypertext Transfer Protocol” which allows the transfer of files that are part of the global network. Their significance is out of scope for this study.

57. *Registering Domain Names*, ICANN (2/13/2025), <https://www.icann.org/resources/pages/register-domain-name-2017-06-20-en> [<https://perma.cc/K73Y-3UTS>].

58. *About Renewing a Domain Name*, ICANN (2/13/2025) <https://www.icann.org/resources/pages/how-2013-05-03-en> [<https://perma.cc/S7UH-329C>].

59. Martin Pramatarov, *What is Domain Name Resolution*, CLOUDNS (Oct. 30, 2024), <https://www.cloudns.net/blog/domain-name-resolution/> [<https://perma.cc/9PDD-P5WM>].

60. See *ICANN Acronyms and Terms*, ICANN, <https://www.icann.org/en/icann-acronyms-and-terms?nav-letter=r&page=1> [<https://perma.cc/Q57B-7HTC>].

61. See *Welcome Registry Operators*, ICANN, <https://www.icann.org/resources/pages/registries/registries-en> [<https://perma.cc/RC49-2NP5>].

Meanwhile, registrars provide domain name registration services to the public based on an accreditation agreement with the relevant registry.⁶² Therefore, the registry serves as the “wholesaler,” managing the master database of all domain names, while the registrar serves as the “retailer,” providing domain name registration services to the public based on an accreditation agreement with the relevant registry.⁶³ In practice, registries such as Verisign⁶⁴ manage TLDs, while registrars such as GoDaddy,⁶⁵ sell SLDs. As such, registrars generally do not host content and may be considered “mere conduit” intermediaries, according to the DSA. However, in practice, many registrars also provide hosting and other services.⁶⁶

Notably, registries⁶⁷ and registrars⁶⁸ enter into an accreditation agreement with ICANN. Contracts between ICANN and registries for TLDs include the terms of the registries’ contracts with domain name registrars. These registry-registrar agreements specify key terms of registrar-domain name registrant contracts.⁶⁹

As for the content, ICANN decides permissible TLDs.⁷⁰ Some TLDs are industry-specific and help clearly define a site’s purpose, such as “.app,” often used by web developers and technology

62. See *ICANN Acronyms and Terms*, ICANN, <https://www.icann.org/en/icann-acronyms-and-terms/registrar-en> [<https://perma.cc/H8TC-TDN8>].

63. *What is a domain name registrar?*, CLOUDFLARE, <https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name-registrar/> [<https://perma.cc/36A7-XMFL>], (“A registrar is like a dealership for domain names, and the registry is like the manufacturer. The registrar facilitates the transactions and provides support services, while the registry is in charge of producing and delivering the goods.”).

64. See *Who We Are*, VERISIGN (2025), <https://www.verisign.com> [<https://perma.cc/Z5PQ-H3PH>].

65. See *Domains*, GODADDY, <https://www.godaddy.com/en-in/offers/godaddy> [<https://perma.cc/2BQQ-AKZ6>].

66. See, e.g., *Domains & Hosting*, IONOS, https://www.ionos.com/domains/domain-names?transaction_id=10254d606e14142ad3078d14c57108&itc=RP0VPYQC-XIDLQ6-0Q1429E&ac=OM.US.USt02K418213T7073a&affiliate_id=6810&utm_source=Forbes+Marketplace+US&utm_medium=affiliate&utm_campaign=AFF-US-DOM-CTLD-6810---&utm_content= [<https://perma.cc/KV8T-X3VL>]; See also *Web Hosting*, GODADDYINDIA, <https://www.godaddy.com/en-in/hosting/web-hosting> [<https://perma.cc/W3JL-2RDY>].

67. See *Generic Top-Level Domain (gTLD) Registry Agreements*, ICANN, <https://www.icann.org/en/registry-agreements> [<https://perma.cc/X5LA-NPHV>].

68. See *Registrar Accreditation Agreement (RAA) & Related Materials*, ICANN, <https://www.icann.org/resources/pages/registrars/registrars-en> [<https://perma.cc/AV86-VZVZ>].

69. See *Signposts in Cyberspace: The Domain Name System and Internet Navigation*, NAT’L RESEARCH COUNCIL OF NAT’L ACAD., at 136-38 (2005) (explaining the relationship between registries, registrars, registrants and the ICANN).

70. See A. Michael Froomkin, *Almost Free: An Analysis of ICANN’s ‘Affirmation of Commitments*, 9 J. ON TELECOMM. & HIGH TECH. L. 187, 211 (2011) (“ICANN can make visible and usable--or nearly invisible and largely useless--TLDs such as .com or .ibm.”).

companies, or “.blog,” popular among bloggers and content creators.⁷¹

Moreover, some scholars have noted “the initial grant of a domain name is usually content-based, if only because two applicants cannot have the same domain name.”⁷² However, once a domain name has been registered, the DNS should not refuse to resolve it because of the content appearing on a site or a chosen domain name.⁷³

B. No Content Flows Through DNS

Once users have registered domain names, they can communicate with each other. This communication, facilitated by the DNS infrastructure, is a multistep process.

In this process, the plain language web address (e.g., ebay.com or berkeley.edu) is translated into an IP by a recursive DNS server, retrieving the relevant information and then sending it back to the initial requester.⁷⁴ Importantly, DNS name servers that resolve DNS queries lack visibility into how the requesting computer uses the returned IP address, let alone the content provided by the host at that address.⁷⁵

Therefore, the function of DNS infrastructure is not to provide content, but a letter-based format-to-IP address translation system to locate content. It operates in a non-intrusive manner, often called the “phonebook” of the internet, allowing people to quickly look up domains.⁷⁶

71. See, e.g., Jelena Laketić, *Trademarks on the Blockchain: NFT Domains and Collisions*, 30 MICH. TECH. L. REV. 1, 19 (“The general idea is that having all these different domains can help internet users communicate information about websites through their domain names more appropriately.”). For the full list of TLDs, see *List of Top-Level Domains*, ICANN, <https://www.icann.org/resources/pages/tlds-2012-02-25-en> [<https://perma.cc/BMC7-9PXN>].

72. Balkin, *supra* note 4 at 2039.

73. *Id.*

74. Moses Musinde, *How DNS Works?*, MEDIUM (Jan. 12, 2023), <https://medium.com/@musinde/how-dns-works-95f2a510eb36> [<https://perma.cc/35SV-FSEU>].

75. See, e.g., Jeremy Malcom et al., *Fighting Neo-Nazis and the Future of Free Expression*, ELEC. FRONTIER FOUND. (Aug. 17, 2017), <https://www.eff.org/deeplinks/2017/08/fighting-neo-nazis-future-free-expression> [<https://perma.cc/89TP-SKT8>] (“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. Registrars’ interests as speakers under the First Amendment are minimal.”).

76. See e.g., Mark Grabowski, *Should the U.S. Reclaim Control of the Internet? Evaluating ICANN’s Administrative Oversight Since the 2016 Handover*, NEB. L. REV. BULL. Aug. 6, 2018 at 3 (“ICANN acts as the phonebook of the Internet by assigning and

Notably, courts in Europe have recognized these characteristics of the DNS before the adoption of the DSA. A Swedish District Court⁷⁷ and a Court of Appeal⁷⁸ ruled that the registry only has an administrative role and acts in the public interest and is thus not obligated to check the legality of website content.

Because of its technical characteristics neither registries, registrars, nor DNS resolvers can intervene in individual content on a website. Their only capability is to suspend a domain name.⁷⁹ When a domain name is suspended, it means that when a user types it into her website browser, it will not resolve or bring the user to the website, essentially making the website invisible on the internet.⁸⁰ However, domain names should not be suspended, for example, based on allegations of political advocacy, nor should they target journalistic content. Such actions can easily lead to censorship of online content.

C. DNS is Private

Internet infrastructure, including the DNS, is primarily held in private hands. Since the US Department of Commerce relinquished its control over ICANN in 2016, allowing the transition to a global multi-stakeholder governance model, ICANN has become almost entirely private.⁸¹ Even though ICANN is still US-based, the private censorship alone does not raise constitutional concerns in the US, as the Supreme Court has consistently ruled that the First Amendment applies only to government actions.⁸²

matching domain names with IP addresses.”); Cf. Adam Thierer, *Soft Law in U.S. ICT Sectors: Four Case Studies*, 61 JURIMETRICS 79, 91 (2020) (“The DNS is often conceptualized as the internet’s phonebook, but it is actually more sophisticated than that analogy suggests.”).

77. See Tingsratt [TR] [Stockholm District Court] 2015-05-19 B 6463-13 (Swed.).

78. See Hovratt [HovR] [Svea Court of Appeal], 2016-05-12, B 5280-15 (Swed.).

79. See generally *Understanding Domain Name Suspension: Causes and Restoration Methods*, MEDIUM (Apr. 10, 2024), <https://medium.com/@wewphosting/why-domains-get-suspended-and-how-to-restore-them-0bc2421d8a2e> [<https://perma.cc/H9K3-R6RN>].

80. *Id.*

81. See *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*, ICANN (Oct. 1, 2016), <https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en> [<https://perma.cc/735T-7CR2>]; See also *ICANN’s Historical Relationship with the U.S. Government*, ICANN, <https://www.icann.org/en/history/icann-usg> [<https://perma.cc/D624-9LLY>].

82. See Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintended Experience*, 78 GEO. WASH. L. REV. 697, 699 (2010) (“Under current law,

The First Amendment, in this context, acts as a negative right, protecting private entities from undue interference by public authorities.⁸³

However, the status of private entities in relation to freedom of expression is a significant area where the US approach differs from EU standards. Unlike the US, the EU adopts a different approach to freedom of expression. In the EU, positive obligations are responsibilities for states to proactively contribute to freedom of expression, instead of merely refraining from intervention.⁸⁴ In this context, the EU's DSA presents a particularly concerning approach compared to the US system, potentially leading to unforeseen risks and challenges. To the extent that the DSA promotes content moderation within the infrastructure layer of the internet, states should play an active role in this process.

Some scholars already argued that governments could potentially coerce or co-opt private entities to aid in speech regulation and surveillance, thereby identifying speakers and sites that the government seeks to monitor, regulate, or shut down.⁸⁵

Notably, the DSA framework draws on fundamental rights.⁸⁶ However, the DSA has its flaws. On the one hand, content moderation is defined broadly.⁸⁷ On the other hand, scholars have noted that many provisions are vague.⁸⁸ Moreover, there are 664

the First Amendment only restricts the actions of state actors and does not restrict the actions of private actors.”); *See also* ERWIN CHEREMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 569 (7th ed. 2023) (“The Constitution applies to government at all levels- federal, state and local- and to the actions of government officials at all levels. The Constitution, however, generally does not apply to private entities or actors.”).

83. *See generally* David P. Currie, *Positive and Negative Constitutional Rights*, 53 U. CHI. L. REV. 864 (1986).

84. *See* Jelena Laketić, *Sterilized Speech: The U.S. Impacts of E.U. Digital Service Rules*, 73 CLEV. ST. L. REV. 1079 (2025).

85. *See* Balkin, *supra* note 15, at 2298 (“To the extent that the government does not own the infrastructure of free expression, it needs to coerce or co-opt private owners to assist in speech regulation and surveillance — to help the state identify speakers and sites that the government seeks to watch, regulate, or shut down.”).

86. DSA, *supra* note 24, at recitals 3, 9, 22, 36, 39-42, 47, 51-54, 63, 154-156.

87. *Id.* at 42-44 (art. 3 (t)) (“[C]ontent moderation’ means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetization, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient’s account.”).

88. *See e.g.*, Husovec, *supra* note 36. *See also* Andrea Palumbo, *A Medley of Public and Private Power in DSA Content Moderation for Harmful but Legal Content: An Account of Transparency, Accountability and Redress Challenges*, 15 J. INTELL. PROP.

million internet domains worldwide.⁸⁹ To handle the enormous traffic, DNS intermediaries would have to develop automated techniques to perform determinations and classify content to make qualitative assessments, even when they are meant to be content agnostic. In other words, they would need to rely on algorithmic filtering tools.⁹⁰ Following this approach, DNS intermediaries would undertake extensive private enforcement via algorithmic structure and practices.

However, broad provisions and vagueness generally do not mix well with algorithmic use. Algorithmic bias is a pervasive and well-documented issue in content moderation.⁹¹ Therefore, content moderation at the DNS level can be disproportionate and affect access to content and services.

III. PROBLEMS WITH INFRASTRUCTURE CONTENT MODERATION

As noted, intermediaries at the internet’s core structure are much further away from content than their hosting and online platform counterparts. However, the technical ease with which domain name suspension can be accomplished is a significant factor that attracts those who support core infrastructural intermediaries to join the content moderation game.

Furthermore, ICANN’s central control of the DNS has the potential to significantly restrict or enhance certain content. This is possible through the power to award or deprive TLD or regulate the performance of domain name registrants or registries, thereby influencing the internet’s content landscape.

INFRO. TECH. & ELEC. COM. L. 246, 250 (2024) (noting that the scope of application of some articles and some key terms are vague).

89. *How Many Domains Are There? Us & Worldwide (2025 Stats)*, HOSTINGADVICE.COM (Jan. 31, 2024), <https://www.hostingadvice.com/how-to/how-many-domains-are-there> [<https://perma.cc/F4RC-PZSS>].

90. See Kate Klonick, *supra* note 1 at 1636 (“The vast majority of [content]... moderation is an automatic process run largely through algorithmic screening without the active use of human decisionmaking.”).

91. See e.g. Solon Barocas & Andrew Selbst, *Big Data’s Disparate Impact*, 104 CALIF. L. REV. 671, 684 (2016) (“Even a dataset with individual records of consistently high quality can suffer from statistical biases that fail to represent different groups in accurate proportions.”); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4 (2014) (“Because human beings program predictive algorithms, their biases and values are embedded into the software’s instructions. . . .”); Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. LEGAL ANALYSIS 1, 4 (2018) (“The reliance on data does not provide algorithms a presumption of truth; the data they are fed can be biased, perhaps because they are rooted in past discrimination...”). See also Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 6–11 (2018).

With its significant role in ensuring the stable and secure operation of the internet's addressing systems, ICANN has consistently resisted pressure to moderate legal content directly. However, even though it sits atop the DNS governance hierarchy, ICANN has not punished some registrars and registry operators for abstaining from moderating content, even when it includes offensive, but legal content.⁹² This Part will explain that, more recently, there has been increasing momentum to regulate online content through the DNS, even within ICANN's multistakeholder governance frameworks. It is crucial to be mindful of the potential for misuse of power by private domain name actors. Because these entities have the ability to ban users from the internet based on the expressive content of their websites, they could inadvertently create tools of censorship.⁹³ These tools could be exploited to suppress other viewpoints or causes, such as political dissent, social activism, or minority rights advocacy.⁹⁴

Moreover, given the speed and scale of online content, and the number of registered domain names, content moderation would become a burdensome and costly task. Therefore, it is beneficial for the EU to transfer the substantial costs of online content moderation to online intermediaries.⁹⁵ Its tiered system of obligations emphasizes that risk should be allocated to the actor who is considered best suited to avoid it.⁹⁶ From the EU perspective, ICANN could reduce these costs because it plays crucial role in allocating IP address space to registries, assigning protocol identifiers, and managing global TLD systems. This transition represents what Balkin called "complicated forms of public/private cooperation"⁹⁷ and marks a notable shift in intermediary regulation

92. See generally Bridy, *supra* note 8 (explaining the content moderation enforcement program between the Motion Picture Association of America (MPAA) and two registry operators, Seattle-based Donuts and Abu Dhabi-based Radix). See also Nugent, *supra* note 8, at 73 (noting that many registrars included so-called "morality clauses" in their acceptable use policies prohibiting registrars from engaging in certain content and explaining how some of those restrictions are not defined and lack standards).

93. Manel Medina, *Governmental Censorship of the Internet: Spanish vs. Catalans Case Study*, 68 LIBRARY TRENDS 561, 568 (2020) ("[T]he Catalan government denounced the abuses and censorship in relation to Internet access committed by Spanish authorities, with the seizing or blocking of more than two hundred web pages related to the self-determination referendum on Catalonia.").

94. See Froomkin, *supra* note 70 at 211 ("...ICANN can make visible and usable—or nearly invisible and largely useless—TLDs such as .com or .ibm.").

95. See e.g., Tarleton Gillespie, *Platforms are Not Intermediaries*, 2 GEO. L. TECH. REV. 198, 198 (2018) ("Content moderation is such a complex and laborious undertaking, it is amazing that it works at all...").

96. See DSA, *supra* note 24 at 44-45, 48, 50-51 (art. 4(1), 5(1), 6(1), 11, 16).

97. Balkin, *supra* note 15, at 2306.

from liability to responsibility. Both phenomena bring significant, negative consequences, which are detailed in the following sections.

A. States Coopting DNS Within Multistakeholder Community

ICANN's central control of the DNS, if not carefully managed, could lead to the misuse of this sophisticated ecosystem for content regulation. ICANN's bylaws serve as a crucial check on its contracting power. The bylaws expressly state that "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide..."⁹⁸ This provision is a key safeguard against the potential misuse of the DNS in content moderation.

Despite this restriction, it would be a fallacy to say DNS intermediaries have not stepped in on content moderation. The truth is that several existing registry contracts have already started to regulate content.⁹⁹ Recently, scholars warned about DNS intermediaries moderating copyright content,¹⁰⁰ offensive content, and hate speech.¹⁰¹ Some DNS intermediaries have also developed cooperation agreements to implement "trusted notifiers" systems for the purpose of reporting abusive content.¹⁰²

While commentators have vehemently criticized this "private censorship,"¹⁰³ the question remains of how this has been made possible. Especially considering ICANN's limited mission focused on the DNS's functionality and its commitment to not using the DNS to regulate content, the existence of private censorship is

98. See Article 1, §1.1(c), ICANN, <https://www.icann.org/resources/pages/governance/bylaws-en/#article1> [<https://perma.cc/88PV-HD7L>] (bylaws as amended Nov. 17, 2023).

99. See e.g., Nugent *supra* note 8 at 73-80 (explaining how certain DNS intermediaries restricted some legal content).

100. See Bridy, *supra* note 8 at 1347 ("Although ICANN has continued to resist direct involvement in copyright enforcement activities, it accommodated right holders in 2013 by altering its contracts with DNS intermediaries to support a system of extra-judicial, notice-driven sanctions.").

101. See Nugent, *supra* note 8 at 45-47.

102. See Bridy, *supra* note 8, at 1371-73.

103. Corynne McSherry et al., *Private Censorship Is Not the Best Way to Fight Hate or Defend Democracy: Here Are Some Better Ideas*, ELECTRONIC FRONTIER FOUNDATION (Jan. 30, 2018), <https://www.eff.org/es/deeplinks/2018/01/private-censorship-not-best-way-fight-hate-or-defend-democracy-here-are-some> [<https://perma.cc/9K6X-VFMH>]; See also Mitch Stoltz, *MPAA May Like Donuts, but They Shouldn't Be the (Copyright) Police*, ELECTRONIC FRONTIER FOUNDATION (Feb. 10, 2016), <https://www.eff.org/deeplinks/2016/02/mpaa-may-donuts-they-shouldnt-be-copyright-police> [<https://perma.cc/DM27-TGVQ>] ("Taking away a website's domain name means interrupting all of the speech that takes place on that site. It creates a much greater danger of censorship than suppressing individual pages or files.").

concerning.¹⁰⁴ The answer to this puzzle lies in the significant influence of national governments within ICANN a factor that often goes unnoticed but plays a crucial role in shaping the organization’s decisions.

1. Registry Voluntary Commitments

ICANN’s complex bureaucracy consists of advisory committees, supporting organizations, working groups, review teams, and task forces.¹⁰⁵ Therefore, the policy specifications come from the multistakeholder community in a process representing a broad set of stakeholders.

Recognizing that restricted use of TLD space was detrimental to entities’ ability to create digital identities and “paving the way for an expansion of domain name choice and opportunity,” ICANN’s Board occasionally expands the number of TLDs.¹⁰⁶ In 2012, during a round of TLD additions, Public Interest Commitments (PICs) emerged now called “Registry Voluntary Commitments.”¹⁰⁷ Developed to appease ICANN’s Governmental Advisory Committee (GAC), which represents the voice of national governments,¹⁰⁸ these require the registry operator to abide by the commitments it made in its application and may also include specific commitments tailored to the TLDs. The problem is that these are not just registry policies of a technical nature.

As Milton Mueller argued, Registry Voluntary Commitments are complex and diverse because they could be about anything.¹⁰⁹

104. See Article 1, §1.1(c) *supra* note 98.

105. See Emily M. Weitzenboeck, *Hybrid Net: The regulatory framework of ICANN and the DNS*, 22 INT’L J. L. & INFO. TECH. 49, 50 (2014) (discussing ICANN’s complex structure).

106. See *Biggest Expansion in gTLDs Approved for Implementation*, ICANN (June 26, 2008), <https://www.icann.org/en/announcements/details/biggest-expansion-in-gtlds-approved-for-implementation-26-6-2008-en> [<https://perma.cc/66XV-JEGZ>].

107. *Public Interest Background*, ICANN, <https://atlarge.icann.org/topics/public-interest/background> [<https://perma.cc/UAN5-XKDD>] (last visited March 26, 2025). See also *Public Interest Commitments, Registry Voluntary Commitments, and Community Registration Policies*, ICANN, 2 n. 3 <https://itp.cdn.icann.org/en/files/policy-development/topic-9-rvcs-pics-14-02-2025-en.pdf> [<https://perma.cc/62J2-FB7G>] (“In the Registry Agreements between ICANN and existing registry operators from the 2012 round of the New gTLD Program, the terms “Registry Voluntary Commitments” and “RVCs” did not exist and instead, the term “specific public interest commitments” was used (the terms “voluntary PICs” and “private PICs” were also used informally in the past).”).

108. *ICANN Governmental Advisory Committee (GAC)*, ICANN, <https://gac.icann.org> [<https://perma.cc/6XWH-ZH8P>] (last visited March 24, 2025).

109. See Milton Mueller, *The Big Question Facing ICANN’s Contractual Governance Regime*, INTERNET GOVERNANCE PROJECT (June 15, 2023), <https://www.internetgovernance.org/2023/06/15/the-big-question-facing-icanns-contractual-governance-regime> [<https://perma.cc/6CYS-JZPL>].

A registry hoping to avoid objections from religious conservatives could promise to banish all blasphemy. A registry hoping to enter the China market could tack on a commitment never to allow any websites that mention the June 4 Tiananmen Square incident, or never allow any reference to the Hong Kong protests. A registry seeking to avoid objections from [the] intellectual property lobby could promise to give copyright owners special powers to monitor or take down domains.¹¹⁰

Likewise, the more open DNS intermediaries are to moderating certain content, the more categories of content intermediaries will be under pressure to moderate.¹¹¹ In this context, the platforms' experience may serve as a warning. It is documented that once the platforms began voluntarily cooperating with EU regulators to remove terrorist propaganda, the scope of prohibited material expanded to other categories including "expression that does not violate existing European law."¹¹²

Moreover, the effort to regulate content through the DNS is not only gaining momentum but also becoming increasingly organized. The ICANN's Governmental Advisory Committee (GAC) openly supports increased contract obligations to moderate content.¹¹³ GAC even goes a step further aiming to make Registry Voluntary Commitments a contractual obligation by incorporating them into the registry contract and having them enforced by the ICANN.¹¹⁴

Through utilizing a sophisticated contractual structure in which the registries commit voluntarily to running their registration policies in a certain way and simultaneously contracting with ICANN to run the registry in a certain way, the

110. *Id.*

111. See Bridy, *supra* note 8, at 1361.

112. Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1039 (2018); see also Balkin, *supra* note 4, at 2040 ("Once the telecommunications system, the DNS system, and the system of electronic payments begin blocking, censoring, or discriminating against certain speakers, nation-states will attempt to piggyback on their technical capabilities. As we have seen, state pressure on infrastructure owners to surveil, block, and filter content creates predictable problems of collateral censorship and privatized prior restraint.").

113. GOVERNMENTAL ADVISORY COMMITTEE, GAC COMMUNIQUÉ – WASHINGTON D.C., UNITED STATES OF AMERICA (2023), <https://gac.icann.org/advice/communiqués/icann77-washington-d-c-communique-zh.pdf> [https://perma.cc/37YR-B7RP].

114. ICANN BUSINESS CONSTITUENCY, COMMUNITY CONSULTATION ON PICs/RVCs BOARD STATEMENT, (Feb. 23, 2024), https://cbu.memberclicks.net/assets/docs/positions-statements/2024/2024_02February_23_BC%20response%20to%20Board%20questions%20on%20RVCs%20and%20PICs.pdf [https://perma.cc/BK3A-HZVN].

GAC argues that ICANN will not be involved in content moderation.

However, considering ICANN's responsibilities to act in the public interest, this argument carries a notable weight. In GAC's words, it "does not amount to ICANN regulating content, merely enforcing an undertaking of specific, objective and measurable processes and procedures, that a registry operator has promised to implement specifically to enforce their RVC."¹¹⁵ Instead, supported by the SubPro PDP Working Group,¹¹⁶ GAC suggested an independent third party monitor and evaluate the registry operator's compliance with a commitment to limit permissible content in SLD registrations.¹¹⁷

The crux is that the GAC initiative would transform ICANN into an enforcer of policies designed to regulate internet content and services. But, ICANN can enforce its contracts only if they are consistent with its mission limitations, and content moderation is certainly inconsistent with its bylaws.

2. ICANN's 80th meeting

In the above explained scenario, the registry operator would agree to remedy violations of content-restrictive commitments identified by the third-party monitor. ICANN would retain enforcement rights concerning the registry operator's failure to comply with the third party's directions. Therefore, if GAC or other influential players condition approval of domains on registries' promises to regulate the content of the domains, ICANN would have to enforce those commitments.

In the face of this challenge, the ICANN Board decided that its bylaws do not allow it to enforce contractual commitments

115. *Id.* at 6.

116. *Id.* at 8.

117. ICANN | GNSO, FINAL REPORT ON THE NEW GTLD SUBSEQUENT PROCEDURES POLICY DEVELOPMENT PROCESS, 49–50 (Feb. 1, 2021), <https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtdl-subsequent-procedures-pdp-02feb21-en.pdf#page=38> [https://perma.cc/V4WD-QEXW] ("To the extent that some registries will want to make voluntary commitments in response to public comments, Government Early Warnings, GAC Advice, etc., it is understood by the Working Group that having these commitments reflected in Registry Agreements even if they fall outside of ICANN's core mission is consistent with the Bylaws where neither ICANN itself nor any third party under ICANN's control is required to pass judgment on 'content'. In such cases, it is understood that using an independent third party as an arbiter to determine whether there has been a violation of the commitment would be consistent with ICANN's mission even if ICANN were ultimately required to rely on that third-party decision to enforce a pre-arranged contractual remedy, which could include sanctions and/or termination of the Registry Agreement.").

involving content moderation.¹¹⁸ The Board noted that even though Section 1.1(d)(v) provides for ICANN’s “ability to enter into and enforce agreements,” it does not shield it “from needing to critically evaluate the substance and impact of those agreements to ensure that the obligations contained in such agreements are reasonably necessary to enable ICANN to pursue its Mission of ensuring the stable and secure operation of the Internet’s unique identifier systems.”¹¹⁹

Moreover, regarding the proposed independent third-party monitor scenario, the Board noted that “the third party would serve as a finder of fact regarding the existence of a breach, but ultimately it would be ICANN – and not the third party – that would take enforcement action based on the registry operator’s failure to remedy the violation...”¹²⁰

With this decision, ICANN reinforced its role in internet infrastructure while protecting users’ fundamental rights to freely express themselves. If ICANN were to enforce the commitments using its contractual compliance regime, it would be fully responsible for content moderation in circumvention of its bylaws. Such a large task could pose significant challenges leading to potential conflicts with its core mission.

B. DSA co-opting DNS

ICANN’s Board made a significant decision in defending against internal government structures attempting to co-opt DNS for online content moderation. However, the potential impact of the DSA on DNS moderation remains the central concern. DNS service providers must be able to provide their services without excessive liability regimes, ensuring the public does not suffer from the chilling effects caused by uncertain policies. Yet, the DSA is lacking in several respects. It is not sufficiently specific and is potentially overbroad, not reflecting the technical functioning of the DNS and thus, opening the way to legal uncertainty and differing legal interpretations.

For instance, DSA is not specific regarding its scope of applicability to “[DNS] services, top-level domain name registries [and] registrars...”¹²¹ In fact, it only mentions them but does not

118. See ICANN, *Approved Resolutions | Regular Meeting of the ICANN Board*, (June 8, 2024), <https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-regular-meeting-of-the-icann-board-08-06-2024-en> [https://perma.cc/2LX2-UU5P].

119. *Id.*

120. *Id.*

121. DSA, *supra* note 24, at recital 28.

define them. This raises several questions as the DSA could potentially apply to ICANN's operations and other actors in the DNS ecosystem.

As previously noted, the DSA only mentions internet infrastructure services in the context of benefiting from the liability exemption rules.¹²² Recital 28 says that DNS services should be included in the DSA's scope of application but only to the extent that they qualify as "intermediary services" defined in Article 3 (g).¹²³ However, no further clarification is given that could help classify DNS services within the intermediary services categories.

Moreover, the recital adds another layer of confusion and is further diluted because it indicates that services are only included "as the case may be."¹²⁴ Therefore, the DSA lacks clarification that could help classify DNS services within existing categories of intermediary services. This indicates that a thorough assessment of applicability for each DNS service is required.

Indeed, the DSA itself recognizes that its technical functionalities may evolve, and what constitutes a mere conduit service, a caching service, or a hosting service must be assessed on a case-by-case basis.¹²⁵ The need for clear and unambiguous regulation is crucial.

Likewise, it is not clear whether the DSA would exempt a registry or registrar from liability for the contents transmitted by a third party. If this were the case, the scenario would become even more complicated. As I have discussed in greater depth in another article, in the EU, there is an important interplay between the DSA horizontal framework and sector-specific legislation.¹²⁶ The EU recently adopted several sectoral rules—the Directive on Copyright

122. DSA, *supra* note 24, at recitals 28, 29.

123. See DSA, *supra* note 24, at art. 3(g) (explaining that intermediary service "means one of the following information society services:

(i) a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

(ii) a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

(iii) a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service.").

124. DSA, *supra* note 24, at recital 28.

125. DSA, *supra* note 24, at recital 29.

126. See Laketić, *supra* note 84, at 1084-1087.

in a Digital Single Market (CDSM Directive),¹²⁷ the Audiovisual Media Services Directive (AVDM),¹²⁸ and the Terrorism Online Content Regulation (TERREG).¹²⁹ Therefore, intermediaries are expected to analyze multiple pieces of legislation to assess the legality of the content ranging from copyright and audiovisual to potential terrorism content. The lack of clarity in the DSA could lead to misinterpretations and potential issues in its application.

Furthermore, as already noted, the DNS ecosystem is complex. DNS can be seen as an address book of the internet consisting of a unique set of names through which domain name resolvers can direct users to the appropriate content online. However, the DNS ecosystem is not straightforward, it consists of various components, including domain name registries and registrars. Domain name registrars act as intermediaries between the registrants—those who wish to secure a domain name—and the registries that maintain the databases of these domain names.

It is unclear whether domain name registrars, who play a crucial role in passing DNS requests from DNS registrants to the registries, should be considered mere conduit services under the DSA.

Similarly, a domain name registration involving both registries and registrars entails minimal information storage, which could be relevant to Article 6 on hosting activities.¹³⁰

As if these aspects were not complex enough, this scenario could be further complicated. For example, to benefit from the liability exemptions, the service in question must be considered one of the intermediation services and an information society service.¹³¹

127. *See generally* Directive 2019/790, of the European Parliament and of the Council 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC O.J (L 130) 92 [hereinafter CDSM].

128. *See generally* Directive 2018/1808, of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of Audiovisual media services [hereinafter AVDSM].

129. *See generally* Commission Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing The Dissemination of Terrorist Content Online, 2021 O.J. (L. 172), 79 [hereinafter TERREG].

130. *See DSA, supra* note 24, at art. 6(1). (“Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider:

- (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or
 - (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.”).
131. *See DSA, supra* note 24, at art. 4-6.

An information society service is “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient.”¹³² But the remuneration criterion introduces a layer of complexity. For instance, users paying registration and renewal fees for domain name services satisfy this criterion. However, not all DNS actors, such as server operators who do not charge for DNS queries, accept remuneration. Their lack of remuneration may exclude them from the definition of information society services, thereby limiting their access to liability exemptions.

Finally, the DSA, with its broad application, presents a complex terrain regarding its territorial applicability.¹³³ Content can be on one or more servers in the same country as the content provider and the content user. However, the provider and the user consuming the content may just as easily be in different jurisdictions, highlighting the global nature of the issue. Moreover, the content itself might be hosted in yet another geographical region with its own laws. This complexity underscores the critical need for a comprehensive legal solution to address the challenging issues of internet jurisdiction and extraterritoriality. ICANN, with its narrow technical mandate, is not equipped to resolve these issues.

C. Why DNS Should Not Engage In Content Moderation

Whether the push for content moderation stems from the internal dynamics of DNS governance or from external regulation, the push carries negative consequences. Balkin’s argument, while not explicitly focused on the DNS system but on the broader internet infrastructure, highlights three key reasons why the internet infrastructure should steer clear of content moderation.¹³⁴ These reasons include a nontransparent and severe lack of due process, the potential harm to content that deserves protection, and the significance of these services for unpopular speakers, which emphasizes the potential impact of DNS content moderation on freedom of expression.¹³⁵

Due process may be hindered by DNS involvement in content moderation. For example, Birdy believes that “privately administered blocking of entire Internet domains raises serious

132. See DSA, *supra* note 24, at recital 5.

133. See DSA, *supra* note 24, at art. 2.

134. See Balkin, *supra* note 4, at 2038-39.

135. *Id.*

issues relating to transparency, fair process, and freedom of expression.”¹³⁶

Moreover, the technical aspects of how DNS works must be considered for a comprehensive understanding of the topic and these concerns. The DNS ecosystem is too remote from content to argue that it should play any role in policing online content.¹³⁷ We do not expect telephone companies to disrupt service based solely on their suspicion that a subscriber is engaged in illegal activity, or states to close roads on which trucks carry contraband.¹³⁸

Because DNS intermediaries do not know about any illegal content, they would need to investigate how domain names are used. Likewise, because DNS intermediaries do not have control over the content, they can only suspend or cancel a domain name.

However, the suspension of domain names presents a significant potential for collateral censorship, lacking transparency, notice, and due process.¹³⁹ Domain names play a crucial role in free expression and dissent, both internally through the website’s content and externally through the diverse “suck sites” on the web (e.g., www.starbucked.com and donaldtrump.sucks). But there is a high risk to silencing political dissent and minority views.

There are also significant proportionality issues concerning the measures DNS actors can employ to moderate content. Unlike intermediaries that moderate individual profiles, DNS targets would not always be individual files or URLs but entire domains. Therefore, the precision of domain related measures is low and the risk of content over blocking is high. For example, suspension could affect all content to which a domain name points, which could be extremely broad. In one instance, the FBI shut down 84000 domain names while the target was just ten.¹⁴⁰

Domain name intermediaries possess the capability to implement filtering technologies aimed at blocking access to websites linked to illegal activities. However, reliance on such

136. Bridy, *supra* note 8, at 1378. *See also* Nugent, *supra* note 8, at 68 (“[A]s private actors, registrars are not well-positioned to determine the legality of registrants’ behavior.”).

137. DeNardis, *supra* note 14, at 619 (citing *Nadel v. N.Y. Tel. Co.*, 170 N.Y.S.2d 95, 96–98 (N.Y. Sup. Ct. 1957)). *See also* MUELLER, *supra* note 51, at 201 (“A true ‘technical coordinator’ role implies that ICANN would be indifferent to any social goals other than its fundamental one of maintaining the global uniqueness of domain names and hence the interoperability, stability, and security of the domain name and addressing systems. This implies neutrality with respect to social outcomes unrelated to that basic mission.”).

138. Nicholas J. Nugent, *The Five Internet Rights*, 98 WASH. L. REV. 527, 619 (2023).

139. *See* Balkin, *supra* note 4, at 2039.

140. Bridy, *supra* note 8, at 1378.

filtering methods often leads to an excessively broad application. In practice, these filtering techniques frequently block all websites on an IP address. Implementing this method results in blocking a significant number of sites unrelated to the alleged wrongdoing.¹⁴¹ This broad approach can lead to considerable disruption, adversely impacting legitimate users and services that play no part in the misconduct being addressed.

DNS content moderation becomes more complex when it comes to lawful but awful content.¹⁴² In this scenario, what is tolerable or not permitted depends on context. Therefore, it is not an easy task for moderators. For instance, a moderator's viewing might be brief, leading to a potential error in their assessment. Furthermore, the moderator might not even be aware of the illicit content, as they might have been checking domain names for different purposes. Commentators have expressed concern about the insufficient due process protections often accompanying domain name suspensions.¹⁴³ Even if the moderator does her job properly, the sheer scale of domain names available for checking is enormous, underscoring the impracticality of the current system. As noted, algorithmic tools are not especially helpful, since algorithmic biases are pervasive and well documented.¹⁴⁴

Finally, the effectiveness of content suspension via the DNS infrastructure must be considered. While DNS suspending means that most users will no longer get a valid IP address when looking up the domain name, it does not eliminate the content from the internet, it just removes the signpost.¹⁴⁵ When an internet user types a domain name into her website browser, it will not resolve to

141. See e.g., Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 397 (2009) ("Most, if not all, Internet filtering systems will be overbroad (blocking innocent content), underbroad (failing to block proscribed material), or both."). See also *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004) (explaining how Verizon blocked hundreds of thousands of websites unrelated to the targeted child pornography when it used DNS filtering to block access to a sub-page of the Terraes website. Some of the websites blocked never contained any child pornography, like a Spanish website for geological surveys).

142. See e.g., Nugent, *supra* note 8, at 72 ("Where DNS governance becomes harder to justify is where DNS intermediaries seek to regulate legal content or conduct based solely on moral grounds.")

143. See e.g., Bridy, *supra* note 8, at 1385 ("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.")

144. See generally Barocas & Selbst, *supra* note 91; Kleinberg, *supra* note 91; Melany Amarikwa, *Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color*, 29 RICH. J. L. & TECH. 69 (2023).

145. See e.g., Nugent, *supra* note 8, at 105 ("Unlike domain names, however, IP addresses, once procured, can be held perpetually. Address block holders need not renew their IP addresses or pay ongoing fees in order to maintain their blocks.")

the website. Average internet users may not know they can circumvent this pitfall, but more sophisticated users will still know how to access the content.¹⁴⁶ This situation stresses the complexity and the challenges DNS ecosystems face because providers of illegal content can anticipate the suspension of domain names and take precautionary measures. For instance, they can register multiple domain names under different TLDs in different jurisdictions and let them resolve to the same IP address.¹⁴⁷ They might also use hyperlinks directly linking to the IP address, bypassing the DNS.¹⁴⁸ As a result, the efforts aimed at DNS moderation are disproportionate and not particularly effective.

CONCLUSION

Infrastructure and DNS play crucial roles in the functioning of the internet. ICANN, the steward of the DNS ecosystem, has withstood years of pressure to moderate content from within its multi-stakeholder community. Recently, its Board made a wise decision to uphold the integrity of the internet by refusing to enforce registry voluntary commitments that involve content restrictions, providing reassurance about the direction of internet governance.

On the other hand, the EU's DSA represents the world's most ambitious attempt to address illegal online content. Notably, it is the first regulation to implicate the steward of the internet's essential technical functions for content moderation. Vague and full of ambiguity, the DSA may be seeking content moderation methods where they are difficult to achieve, opening the way to inconsistency and mistakes. It could transform DNS into a potent tool for suppressing the speech of some internet users, including political dissent and minority views.

146. Bridy, *supra* note 8, at 1381.

147. See COUNCIL OF EUROPEAN NATIONAL TOP-LEVEL DOMAINS, DOMAIN NAME REGISTRIES AND ONLINE CONTENT, 15 (2022).

148. *Id.*