Washington Law Review

Volume 98 | Number 2

6-1-2023

The Five Internet Rights

Nicholas J. Nugent
University of Tennessee

THE FIVE INTERNET RIGHTS

Nicholas J. Nugent*

Abstract: Since the dawn of the commercial internet, content moderation has operated under an implicit social contract that website operators could accept or reject users and content as they saw fit, but users in turn could self-publish their views on their own websites if no one else would have them. However, as online service providers and activists have become ever more innovative and aggressive in their efforts to deplatform controversial speakers, content moderation has progressively moved down into the core infrastructure of the internet, targeting critical resources, such as networks, domain names, and IP addresses, on which all websites depend. These innovations point to a world in which it may soon be possible for private gatekeepers to exclude unpopular users, groups, or viewpoints from the internet altogether, a phenomenon I call *viewpoint foreclosure*.

For more than three decades, internet scholars have searched, in vain, for a unifying theory of interventionism—a set of principles to guide when the law should intervene in the private moderation of lawful online content and what that intervention should look like. These efforts have failed precisely because they have focused on the wrong gatekeepers, scrutinizing the actions of social media companies, search engines, and other third-party websites—entities that directly publish, block, or link to user-generated content—while ignoring the core resources and providers that make internet speech possible in the first place. This Article is the first to articulate a workable theory of interventionism by focusing on the far more fundamental question of whether users should have *any* right to express themselves on the now fully privatized internet. By articulating a new theory premised on viewpoint access—the right to express one's views on the internet itself (rather than on any individual website)—I argue that the law need take account of only five basic non-discrimination rights to protect online expression from private interference—namely, the rights of connectivity, addressability, nameability, routability, and accessibility. Looking to property theory, internet architecture, and economic concepts around market entry barriers, it becomes clear that as long as these five fundamental internet rights are respected, users are never truly prevented from competing in the online marketplace of ideas, no matter the actions of any would-be deplatformer.

* Assistant Professor of Law, University of Tennessee (beginning August 2023); Karsh Fellow, Lecturer in Law, Program Director for the Karsh Center for Law & Democracy, University of Virginia School of Law; former Attorney for Microsoft; former Senior Corporate Counsel for Amazon. In addition to Danielle Citron, Fred Schauer, Deborah Hellman, Lawrence Solum, Micah Schwartzman, John Duffy, Paul Edelman, Christopher Yoo, and Rebecca Weitzel, I would like to thank participants in the 2022 Stanford-Penn-Northwestern Junior Faculty Forum for Law & STEM as well as my Internet Regulation seminar students for their thoughtful comments and critiques. The views expressed in this Article are solely my own and do not necessarily reflect the views of any current or former clients or employers.

INTRODUCTION

When, if ever, should the law intervene in how private intermediaries moderate lawful online content? For example, should social media companies like Facebook and Twitter be forced to treat user-generated content in a viewpoint-neutral manner? Or should the law instead empower them to protect users from toxic content by shielding providers from liability for their moderation decisions? Should Federal Communications Commission (FCC) rules prevent internet service

providers like Comcast and T-Mobile from blocking websites critical of their interests, or should they remain free to use their property as they see fit? Should domain name registrars, cloud hosting providers, and payment processors do more to stamp out bigotry and extremism, or are their operations so far removed from user expression that they should be required to stay out of the moderation game completely?

To many in the United States, the answers to these questions might seem obvious. *The state* can't *regulate private content moderation*, some might say, *because the First Amendment vests online providers with "inviolable" editorial discretion*.[1]

Not so, others might respond. *Simply hosting third-party speech doesn't allow a company to escape regulation, especially if it functions like a "sovereign power" or a "private monopoly*."[2]

Still others: *Not only* can *the state weigh into content policy, but if it hopes to protect public health from misinformation, marginalized groups from harassment, and even the electoral process itself from the*

---

1. Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 771 (2010); *see also* Evelyn Douek, *Content Moderation as Systems Thinking*, 136 HARV. L. REV. 526, 532 (2022) ("[I]t is a First Amendment right . . . for platforms to moderate."); Eric Goldman, *Of Course the First Amendment Protects Google and Facebook (and It's Not a Close Question)*, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Feb. 26, 2018), https://knightcolumbia.org/content/course-first-amendment-protects-google-and-facebook-and-its-not-close-question [https://perma.cc/S8NX-TU6Z]; Ashutosh Bhagwat, *Do Platforms Have Editorial Rights?*, 1 J. FREE SPEECH L. 97, 117–23 (2021) ("[I]t seems unexceptional that social media platforms are entitled to First Amendment editorial rights."); Edward Lee, *Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance*, 70 AM. U. L. REV. 913, 1035 (2021) ("Congress could not directly require internet platforms to adopt political viewpoint neutrality (or otherwise to limit their content moderation to only unlawful content) because such a law would violate the internet platforms' own freedom of speech."); Jennifer A. Chandler, *A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet*, 35 HOFSTRA L. REV. 1095, 1125 (2007) ("[R]egulations aimed at controlling the bias introduced by selection intermediaries such as search engines and network operators are vulnerable to the claim that they violate the First Amendment rights of the intermediaries themselves.").

2. Tunku Varadarajan, *The 'Common Carrier' Solution to Social-Media Censorship*, WALL ST. J. (Jan. 15, 2021, 12:39 PM), https://www.wsj.com/articles/the-common-carrier-solution-to-social-media-censorship-11610732343 (interviewing Richard Epstein) (last visited Apr. 8, 2023); *see also* Biden v. Knight First Amend. Inst. at Colum. Univ., 593 U.S. __, 141 S. Ct. 1220, 1223–24 (2021) (Thomas, J., concurring) ("Internet platforms of course have their own First Amendment interests, but regulations that might affect speech are valid if they would have been permissible at the time of the founding."); Eugene Volokh, *Treating Social Media Platforms Like Common Carriers?*, 1 J. FREE SPEECH L. 377, 416 (2021) ("[The Supreme Court] expressly rejected the claim 'that a private property owner has a First Amendment right not to be forced by the State to use his property as a forum for the speech of others.'"); Philip Hamburger & Clare Morell, *The First Amendment Doesn't Protect Big Tech's Censorship*, WALL ST. J. (July 31, 2021, 11:31 AM), https://www.wsj.com/articles/big-tech-twitter-facebook-google-youtube-sec-230-common-carrier-11627656722 (last visited Apr. 8, 2023) ("[L]arge tech platforms and services function as common carriers" for which "[t]he states and the federal government have the power to . . . ban discrimination.").

"worldwide, internet-based assault on democracy,"[3] *it* must *do so by "hold[ing] online platforms accountable" for their content moderation decisions*.[4]

Beneath each of these positions lies a theoretical framework—a *theory of interventionism*—that attempts to explain when the state should intervene in private content moderation and what that intervention should look like. For example, those who wish to protect users from allegedly unfair treatment by social media companies have looked to non-discrimination regimes, such as common carriage or public accommodation laws.[5] Those who would use the law to protect hosting providers when they terminate services to controversial website operators might stake their position on the property rights such providers enjoy in their hardware and software[6] or in Section 230's[7] goal of empowering "good Samaritans" to clean up the internet.[8] And multiple voices in this

3. SIVA VAIDYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 182 (2018).

4. Alexandra S. Levine, *Klobuchar Targets Vaccine Misinformation with Section 230 Bill*, POLITICO (July 22, 2021, 2:13 PM), https://www.politico.com/news/2021/07/22/klobuchar-vaccine-misinformation-section-230-bill-500554 [https://perma.cc/2S9V-K9EL]; *see also* Rebecca J. Hamilton, *Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators to Commit Atrocities*, 63 B.C. L. REV. 1349, 1405 (2022) ("[R]egulatory action that publicly and credibly threatens Meta's profits may be one way to propel the corporation to . . . stop the spread of dangerous speech."); Alvin I. Goldman & Daniel Baker, *Free Speech, Fake News, and Democracy*, 18 FIRST AMEND. L. REV. 66, 125–26 (2019) ("[R]egulation of fake news and false campaign speech is . . . 'necessary' to meet the compelling government interest . . . of preserving the integrity of the election process.").

5. For examples of scholars and commentators who have entertained using non-discrimination laws to regulate online platforms (not including ISPs), see Volokh, *supra* note 2, at 454–60; Hamburger & Morell, *supra* note 2; Varadarajan, *supra* note 2; Adam Candeub, *Bargaining for Free Speech: Common Carriage, Network Neutrality, and Section 230*, 22 YALE J.L. & TECH. 391, 433 (2020); K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234 (2018); Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353, 1366 (2018); David McCabe, *One Idea for Regulating Google and Facebook's Control Over Content*, AXIOS (Aug. 18, 2017), https://www.axios.com/2017/12/15/one-idea-for-regulating-google-and-facebooks-control-over-content-1513304938 [https://perma.cc/VA9J-SGBT].

6. For examples of scholars who have considered property rights as a basis for content moderation (positively or negatively), see James Grimmelmann, *The Virtues of Moderation*, 17 YALE J.L. & TECH. 42, 56 (2015); Adam Thierer, *The Perils of Classifying Social Media Platforms as Public Utilities*, 21 COMMLAW CONSPECTUS 249, 292 (2013); Daniel A. Lyons, *Virtual Takings: The Coming Fifth Amendment Challenge to Net Neutrality Regulation*, 86 NOTRE DAME L. REV. 65 (2011); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 520 (1999).

7. 47 U.S.C. § 230.

8. *See id.* § 230(c); Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 154, 169–70 (Giancarlo Frosio ed., 2020); JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 3–5 (2019); *Liability for User-Generated Content Online: Principles for Lawmakers* (July 11, 2019),

debate have claimed that the First Amendment not only presents no barriers to their proposed interventions but effectively constitutionalizes their position.[9]

Of course, many of these theories are at odds with each other. TikTok cannot simultaneously be immune from state interference *and* be classified as a state actor. Provider property interests inexorably conflict with user property interests. And Good Samaritanism, when practiced by a monopolist, can be just as dangerous to democracy as content anarchism. In the face of such fierce disagreements over policy outcomes, theoretical frameworks, and even conceptions of speech, it might seem that little can be done to find consensus. After all, if scholars and jurists can't even agree on when a private website constitutes a public forum,[10] the prospect of a unified theory of interventionism seems slim.

Yet this Article endeavors to find common ground by offering a simple thought experiment: suppose private actors could successfully exclude an unpopular user, group, or viewpoint from the internet altogether. Should the law step in to prevent *that* outcome? Many scholars, I suspect, would concede that if "content moderation" were to reach that extreme state, then yes, the law should indeed intervene to provide *some* kind of basic right to express oneself online, whatever that might look like.

But at the same time, some might regard such a thought experiment as fanciful, believing that no one could actually be excluded from the internet, short of incarceration or government-enforced censorship. The idea that private service providers could effectively control what could and could not be said throughout the internet seems implausible because alternate providers always exist, at least some of which will agree to host controversial speech rejected by others. And even if such alternate providers could not be found, a true rebel could always create her own website to host her own speech as well as that of likeminded users.

It might come as a surprise, therefore, that certain private operators can, in fact, control which viewpoints are published on the internet, as a whole,

---

https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical [https://perma.cc/P8LW-RHZU]; Annemarie Bridy, *Remediating Social Media: A Layer-Conscious Approach*, 24 B.U. J. SCI. & TECH. L. 193, 219–27 (2018).

9. *Compare* Bhagwat, *supra* note 1, at 117–23 (arguing that "social media platforms are entitled to First Amendment editorial rights" to moderate user content), *with* Vivek Ramaswamy & Jed Rubenfeld, *Save the Constitution from Big Tech: Congressional Threats and Inducements Make Twitter and Facebook Censorship a Free-Speech Violation*, WALL ST. J. (Jan. 11, 2021, 12:45 PM), https://www.wsj.com/articles/save-the-constitution-from-big-tech-11610387105 (last visited Apr. 8, 2023) (asserting a First Amendment right *against* social media "censorship").

10. *See, e.g.*, Biden v. Knight First Amend. Inst. at Colum. Univ., 593 U.S. __, 141 S. Ct. 1220, 1225 (2021) (Thomas, J., concurring) (questioning the Second Circuit's conclusion that then-President Trump's Twitter comment thread constituted a public forum despite the fact that Twitter could terminate the forum at any time).

without any help from the state. Although countless website providers exist—and that diversity generally does ensure that most user-generated content can find a home somewhere—certain *core* internet functions are performed by only a handful of private providers, none of which are meaningfully regulated under U.S. law. Historically, these core providers have been careful to steer clear of debates over content, hewing closely instead to their original charters as neutral stewards of internet stability.

But that neutrality may now be waning. In the aftermath of the January 6th Capitol riot, several obscure developments unfolded that promise to test the boundaries of just how far content moderation can or should go. Following the riot, GoDaddy, the world's largest registrar, suspended the ar15.com domain name after it was alleged that one or more users had posted content on the site celebrating (though not engaging in) violence.[11] That suspension would take down the world's largest online gun forum, making it effectively unreachable on the internet. Days later, in what could only be described as retaliation for the permanent suspension of Donald Trump's social media accounts, an internet service provider in rural Idaho blocked its subscribers from accessing Facebook or Twitter.[12]

Still, the most concerning development centered on Parler, the embattled alternative social network to which many users flocked after being booted from mainstream platforms.[13] While the decision by Amazon Web Services to terminate Parler's cloud hosting services, and thereby take it offline, generated widespread coverage and debate,[14] scarcely any attention was paid to a far more significant event. Shortly after Parler managed to migrate to an alternate host, it went dark again, but this time for a different reason. After complaints reached the Latin America and Caribbean Network Information Centre (LACNIC), one of the five regional internet registries responsible for managing the world's network identifiers, LACNIC revoked more than eight thousand IP addresses used by Parler and its new hosting provider, taking Parler

11. 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/U762-FGLS].

12. Karl Bode, *ISP Blocks Twitter and Facebook to Protest Anti-Trump 'Censorship'*, VICE (Jan. 11, 2021, 10:29 PM), https://www.vice.com/en/article/m7a5ay/isp-blocks-twitter-facebook-protest-trump-ban-censorship [https://perma.cc/J6HN-AMUU].

13. *See* Kari Paul, *Parler: The Social Network That's Winning Conservative Recruits*, GUARDIAN (Nov. 13, 2020, 9:10 AM), https://www.theguardian.com/media/2020/nov/13/parler-conservative-social-network-free-speech [https://perma.cc/3JBP-ZFUP].

14. *See* Alex Fitzpatrick, *Why Amazon's Move to Drop Parler Is a Big Deal for the Future of the Internet*, TIME (Jan. 21, 2021, 3:06 PM), https://time.com/5929888/amazon-parler-aws/ [https://perma.cc/FQK8-S856].

offline once more.[15] A year later, the government of Ukraine sent a similar request to Europe's regional internet registry to revoke IP addresses used by Russian websites that spread propaganda about the war in Ukraine.[16]

These developments portend a new phase in the evolution of content moderation. Whereas previous efforts to deplatform unpopular speakers remained confined to website administration, or even website hosting, new forms of deep deplatforming are now reaching down into the core of the internet's infrastructure. These efforts, and others like them, raise the very real possibility that the complete privatization of the internet, coupled with increasingly innovative forms of deplatforming, may soon produce a world in which the most unpopular viewpoints can be excluded from the internet altogether, a phenomenon I call *viewpoint foreclosure*.

Viewpoint foreclosure would mean the end of a long-assumed—though never legally guaranteed—safety valve for free expression on the internet: that a user whose viewpoints are rejected from every other online forum can always, as a last resort, publish her opinions on her own website and potentially grow an audience if her ideas take hold. Needless to say, the prospect of losing this safety valve challenges our traditional conception of the internet as an open forum for the free exchange of ideas. But it also presents an opportunity. If internet scholars and policymakers can align on a simple theoretical principle—that all users should enjoy a basic right to *self*-publish their viewpoints on the internet—then this humble kernel of consensus can provide the foundation for a broader theory of interventionism centered on *viewpoint access*.

In its most basic form, viewpoint access theory offers a set of minimum rights that would apply to all users. Specifically, when we examine the architecture of the internet, we can discern five fundamental rights that users must enjoy if they are to be secure in their ability to publish their viewpoints online through their own publicly accessible websites:

- **Connectivity:** The right to connect a webserver to the public internet;
- **Addressability:** The right to maintain stable IP addresses to transmit web content to requesting users;
- **Nameability:** The right to make a website reachable via a domain name;

---

15. Brian Krebs, *DDoS-Guard to Forfeit Internet Space Occupied by Parler*, KREBS ON SEC. (Jan. 21, 2021), https://krebsonsecurity.com/2021/01/ddos-guard-to-forfeit-internet-space-occupied-by-parler/ [https://perma.cc/NA4C-FUNK].

16. *See* Letter from Mykhailo Fedorov, Vice Prime Minister & Minister of Digit. Transformation of Ukraine, to Hans Petter Holen, Managing Director, RIPE NCC (Mar. 2, 2022) [hereinafter Federov Letter], https://www.ripe.net/publications/news/announcements/request-from-ukrainian-government.pdf [https://perma.cc/JJ79-9L57].

- **Routability:** The right to have communications faithfully routed between intervening networks; and
- **Accessibility:** The right not to have one's audience blocked from accessing such content by their internet service providers.

But these five internet rights provide only a floor—the mere *technical* ability to publish on the internet—not a ceiling. Therefore, in its more expansive form, viewpoint access theory borrows from economic concepts—in particular, market entry barriers—to offer a framework for evaluating other potential interventions into content moderation. Viewpoint access theory, thus, offers both a limiting principle (when private content moderation goes too far) and a guiding principle (when and how the law should intervene) to inform potential future regulation.

Countless articles, both academic and in popular media, have been penned alternately arguing that YouTube, Reddit, and other popular websites should or should not be forced to host certain kinds of user content or that democracy does or does not depend on whether their acceptable use policies are co-extensive with the First Amendment.[17] This is not one of them. This Article ultimately does not concern itself with whether Twitter "censors" this or that user or whether Facebook's Oversight Board should serve as a model of private governance for other social media companies.[18] Instead, it asks whether Twitter, Facebook, or any other private website should have the right to *exist* in the first place.

This Article makes three contributions to the study of content moderation in general and deplatforming in particular. First, it provides a comprehensive taxonomy of existing interventionist theories. Part I distills the theoretical principles underlying both laws that strengthen providers' rights to discriminate against users and content—from property rights to Good Samaritanism to editorial rights—and laws that grant users the right to access provider systems—from expressive rights to non-discrimination to user property rights. It evaluates the strengths and weaknesses of each such theory before ultimately concluding that none of these theories adequately explains when the law should intervene in

17. *Compare Elon Musk to Acquire Twitter*, PR NEWSWIRE (Apr. 25, 2022, 2:50 PM), https://www.prnewswire.com/news-releases/elon-musk-to-acquire-twitter-301532245.html [https://perma.cc/UY6T-URHP] ("Free speech is the bedrock of a functioning democracy, and Twitter is the digital town square where matters vital to the future of humanity are debated."), *with* Matt Pearce, *Obama Argues Unregulated Social Media Is a Threat to Democracy, Calls to 'Pick a Side'*, L.A. TIMES (Apr. 21, 2022, 6:19 PM), https://www.latimes.com/entertainment-arts/story/2022-04-21/la-ent-obama-disinformation-stanford [https://perma.cc/FR3K-7TJR].

18. For recent thoughtful scholarship on the topic of private governance—how platforms should choose to moderate content in the absence of regulation—see Evelyn Douek, *Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability*, 121 COLUM. L. REV. 759 (2021); Lee, *supra* note 1; Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L.J. 2418 (2020).

private content moderation.

Second, this Article identifies and describes the phenomenon of viewpoint foreclosure. Using the heuristic of a three-layer internet stack, Part II chronicles the evolution of content moderation as it has passed through four distinct stages: classic content moderation, deplatforming, deep deplatforming, and, finally, viewpoint foreclosure. It shows (visually) how each successive stage has pushed content moderation deeper down the internet stack until the most unpopular speakers are left with no viable options to stay online. And it evaluates whether this development is consistent with the historical promise of the internet itself (not any particular website) as an open forum for the free exchange of ideas.

Third, this Article articulates a new theory of interventionism based on viewpoint access, the idea that, at a minimum, the law should intervene to ensure that all users have the opportunity to express themselves online by operating their own publicly accessible websites. Part III evaluates viewpoint access theory by comparing it to each of the existing interventionist theories canvased in Part I and shows how it incorporates the most important principles from these other theories while discarding their flaws. It then explains *how* the law can enforce viewpoint access by guaranteeing five fundamental rights that naturally flow from the architecture of the internet—in particular, the rights of connectivity, addressability, nameability, routability, and accessibility.

Finally, in Part IV, I respond to what I anticipate will be the most common objections to viewpoint access theory and the five internet rights it entails.

I. THE SEARCH FOR AN INTERVENTIONIST THEORY

The history of the "public internet" is one of privatization. Although originally developed and administered by the U.S. Department of Defense and the National Science Foundation, beginning in the 1990s, the internet incrementally transitioned from governmental to private control.[19] Culminating in the Commerce Department's move in 2016 to relinquish control of the Internet Corporation for Assigned Names and Numbers (ICANN),[20] today's public internet is very much a private network, where

19. *See ICANN's Historical Relationship with the U.S. Government*, ICANN, https://www.icann.org/en/history/icann-usg [https://perma.cc/8NSC-37ZU]. Although universities, both public and private, also played a central role in the development of the early internet, ultimate control over the broader U.S. Advanced Research Projects Agency Network (ARPANET) and National Science Foundation Network (NSFNET) projects, as well as the domain name system, remained with the federal government until the mid-1990s. *Id.*

20. *See id.*

private parties act as gatekeepers for who can say what, when, where, how, and to whom.

The privatization of the internet raises important questions when it comes to content moderation. What if network providers block access to content critical of their economic interests? Is the political process harmed if powerful social media companies use their control over what users see to influence elections or public discourse? Should users have no due process rights against platforms that terminate their accounts without notice or opportunity to be heard?

While some believe that free market incentives suffice to mitigate these dangers, others have called for the law to intervene. Proposals for regulating the content moderation practices of online service providers have proliferated in recent years, from classifying hosting companies as common carriers to requiring social media platforms to limit the spread of disinformation. But while these legislative proposals capture the national attention, beneath these debates lies a far more fundamental inquiry. Premising their proposed interventions on everything from non-discrimination to Good Samaritanism to editorial rights, this debate highlights the elusive quest for a *theory* of interventionism, a set of principles or interests that animate not just any one piece of legislation but the broader enterprise of determining when the law should intervene in private content moderation.

This debate remains unsettled, and the quest for an overarching theory remains in progress. Therefore, before attempting to advance my own theory of interventionism, in this Part, I canvas the dominant existing theories, explaining their origins as well as their strengths and weaknesses. Section A first provides a taxonomy of interventionist regulation, placing the positive law along a spectrum from the laissez-faire arena of the common law to the strong interventionism of constitutional rights. Sections B and C then examine and critique prevailing provider-centric and user-centric theories, respectively.

A. A Taxonomy of Interventionist Regulation

Fundamentally, content moderation captures the struggle between two parties. A user—be it an individual or an organization—wishes to leverage an online service provider to publish content or communicate with third parties. Often, the service provider is happy to oblige, and a mutually beneficial economic relationship blooms. But in some cases, whether for economic, moral, or other reasons, a provider might wish instead to block, remove, or de-amplify certain content or, in extreme cases, to terminate services to a disfavored user altogether. It is this perennial conflict between the user's interest in accessing the provider's

services and the provider's interest in controlling access that lies at the heart of content moderation.

In a deregulated environment, or something close to it, users and providers must simply duke it out when they disagree about content or access. Because they control their own hardware, software, or network cables, providers have a natural advantage in this war of interests. Yahoo can block your marketing emails as spam, Instagram can terminate your account, and there's little you can do about it. The common law adds to this advantage in that providers can largely dictate their terms of service, granting themselves the contractual right to terminate access for any reason or no reason.[21] And should a savvy user find a way to access a provider's system without permission, the provider could look to common law property-based claims, such as trespass to chattels.[22]

But a provider's advantage in a deregulated environment is not perfect. Powerful users, such as paying enterprise customers, can negotiate better terms of service. Ancient property doctrines, such as trespass or conversion, map awkwardly to electrical signals sent over public networks where no physical intrusion occurs,[23] and disgruntled users could potentially bring their own property claims against providers for lost content, especially where serious economic hardship results.[24] And even if the common law generally protects providers from their own end users, third parties might nonetheless sue providers for hosting infringing or defamatory content, which might force them to forgo content moderation altogether, lest they be classified as publishers and held strictly liable for the conduct of their users.[25]

Faced with this state of affairs, where most users remain at the mercy of online service providers and where service providers enjoy a significant

---

21. *See, e.g.*, *Terms of Service: Using the Services*, TWITTER (June 10, 2022) [hereinafter TWITTER, *Terms of Service*], https://twitter.com/en/tos [https://perma.cc/S3FP-MBSX] ("We may . . . remove or refuse to distribute any Content on the Services, limit distribution or visibility of any Content on the service, suspend or terminate users, and reclaim usernames without liability to you.").

22. For early examples of cases in which online service providers successfully used common law property-based claims to prevent unauthorized access to their systems, see eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

23. *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (rejecting the claim that a disgruntled ex-employee's unsolicited emails to former Intel coworkers constituted a "trespass" to Intel's email servers); Ticketmaster Corp. v. Tickets.com, No. CV99-7654, 2003 U.S. Dist. LEXIS 6483, at *12 (C.D. Cal. Mar. 6, 2003) (dismissing a trespass to chattels claim based on "deep-linking" into another website).

24. *Cf.* Rory Van Loo, *Federal Rules of Platform Procedure*, 88 U. CHI. L. REV. 829, 841 (2021) (providing examples of online account terminations that "deprive[d] . . . user[s] of valuable property").

25. *See infra* section I.B.3.

but uncertain power advantage over their users, the law has two choices. It can either leave this dynamic in place—the *laissez-faire* approach—or it can intervene by placing a thumb on the scale in favor of the user, the provider, or even the government—the *interventionist* approach.

Laws that favor users over providers—*user-centric interventionism*—generally come in two forms: forced carriage and forced process. Forced carriage laws require providers to host or carry user content they might otherwise block or take down. For example, Florida's S.B. 7072 prohibits social media platforms from "censor[ing]" any "journalistic enterprise based on the content of its publication or broadcast."[26] Other forced carriage laws or policies might require cloud computing providers to host their customers' lawful websites or mobile service providers to allow subscribers to use video conferencing apps of their choice.

Forced *process* laws, by contrast, allow providers to take down content that violates their terms of service but only if they provide certain due process rights to users whose accounts are affected. For example, if a social media platform removes user content because it violates the platform's acceptable use policy, Texas's H.B. 20, requires the provider to explain why the content was removed and allow the user to appeal the decision.[27]

Laws that favor providers over users—*provider-centric interventionism*—operate a little differently. Rather than imposing any obligations on providers, whether carriage or process, these laws empower providers to moderate content as they see fit. Most famously, the 1996 Telecommunications Act[28] includes a provision—commonly referred to as Section 230—that protects providers of "interactive computer services" against certain forms of liability for their decisions to take content down or leave it up.[29]

Thus, when it comes to forced carriage, user-centric laws operate by protecting users' rights to *access* providers' services while provider-centric laws operate by protecting providers' rights to *discriminate* against users or content.

Alternatively, the law could intervene by frustrating both users and providers. Forced *takedown* laws require providers to take down user content they might otherwise leave up. For example, a law targeting revenge porn might force Reddit to take down a nude picture of a third

26. FLA. STAT. § 501.2041 (2022).

27. TEX. BUS. & COM. CODE § 120.103 (2021).

28. Pub. L. No. 101–04, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

29. *See* 47 U.S.C. § 230(c)(2).

party who objects to its distribution,[30] even in situations where the posting user owns the copyright. Or, concerned about the proliferation of fake news or online harassment, legislators have proposed bills that would require certain website operators to take down or de-amplify various categories of toxic or misleading content.[31]

Of course, forced takedown regimes that pertain to lawful content might face steep odds against the First Amendment.[32] And forced process, while likely more constitutionally sound, is the subject of an emerging and increasingly rich body of scholarship,[33] which I do not wade into. Instead, this Article focuses exclusively on the issue of forced carriage. More particularly, it aims to articulate a workable theory of interventionism to address a widely debated question: when, if ever, should the law intervene in how private intermediaries moderate lawful content?

In the United States, this remains an unresolved question. No federal law comprehensively regulates the moderation of lawful content, and, contrary to popular belief,[34] Supreme Court precedent does not clearly indicate what kind of regulation the Constitution would permit. As a result, users and providers currently must rely on a patchwork of other laws, most of which predate the modern internet, to advance their policy preferences. Figure 1 depicts the landscape of existing laws and doctrines

---

30. *See, e.g.*, Maggie Miller, *New Senate Bill Would Allow Victims to Sue Websites that Host Revenge Porn, Forced Sexual Acts*, HILL (Dec. 9, 2020, 5:12 PM), https://thehill.com/policy/technology/529542-new-senate-bill-would-allow-victims-to-sue-websites-that-host-revenge-porn/ [https://perma.cc/VEN7-Y8KV] (describing a proposed federal bill that "would allow . . . victims depicted in sexual imagery made public without their consent[] to sue websites that knowingly host or distribute video or pictures" of such imagery).

31. *See, e.g.*, Bernadette Hogan & Theo Wayt, *New NY Bill Aims to Hold Social Media Companies Accountable for Disinformation*, N.Y. POST (Dec. 26, 2021, 6:08 PM), https://nypost.com/2021/12/26/ny-bill-aims-to-hold-social-media-companies-accountable-for-disinformation/ [https://perma.cc/5K6Y-EHS5] (describing a proposed New York bill that would subject online platforms to private suit for amplifying user-generated content directed to self-harm or vaccine disinformation).

32. *See* Volokh v. James, No. 22-CV-10195, 2023 U.S. Dist. LEXIS 25196 (S.D.N.Y. Feb. 14, 2023) (preliminarily enjoining as unconstitutional a far tamer law requiring social media companies merely to publish policies for how they will respond to complaints of hate speech on their platforms).

33. *E.g.*, Niva Elkin-Koren, Giovanni De Gregorio & Maayan Perel, *Social Media as Contractual Networks: A Bottom Up Check on Content Moderation*, 107 IOWA L. REV. 987, 1044–45 (2022); Van Loo, *supra* note 24; Lee, *supra* note 1; Cindy Cohn, *Bad Facts Make Bad Law: How Platform Censorship Has Failed So Far and How to Ensure that the Response to Neo-Nazis Doesn't Make It Worse*, 2 GEO. L. TECH. REV. 432, 447–50 (2018); JOHN BERGMAYER, PUB. KNOWLEDGE, EVEN UNDER KIND MASTERS: A PROPOSAL TO REQUIRE THAT DOMINANT PLATFORMS ACCORD THEIR USERS DUE PROCESS (2018), https://publicknowledge.org/wp-content/uploads/2021/11/Even_Under_Kind_Masters-4.pdf [https://perma.cc/JHJ6-BGRS].

34. *See, e.g.*, authorities cited *supra* note 1 (taking the position that laws regulating private content moderation are unconstitutional under the First Amendment).

that litigants and scholars have attempted to use or retrofit for modern content disputes.

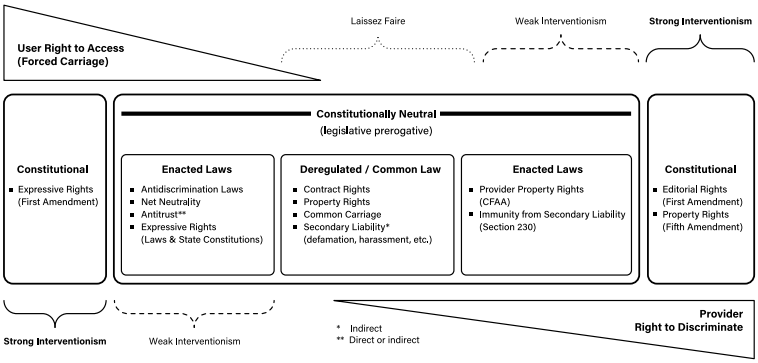

Figure 1 – The Spectrum of Interventionism

As can be seen in Figure 1, and as noted above, in a deregulated (laissez-faire) environment, providers generally enjoy a significant but uncertain power advantage over their users by virtue of their property and contract rights, as mitigated by the risk of being classified as common carriers under the common law or being held secondarily liable for their users' conduct. To bolster their position, therefore, providers must look to enacted laws, including statutes, regulations, and state constitutions. For example, the Computer Fraud and Abuse Act[35] clarifies property rights in computer systems,[36] and Section 230 shields providers from certain forms of secondary liability.[37]

But users are not without their own statutory weapons. Antidiscrimination laws, some have argued, might prevent providers from discriminating against users for various reasons, potentially including their viewpoints.[38] Net neutrality rules, before they were withdrawn, prevented internet service providers (ISPs) from blocking access to lawful content and applications.[39] Antitrust law might impose a duty to serve on large providers that enjoy market power (direct intervention) or perhaps simply help to foster a diverse array of content policies by injecting more

35. 18 U.S.C. § 1030.
36. *See infra* section I.B.2.
37. *See infra* section I.B.3.
38. *See infra* section I.C.2.
39. *See id.*

competition into the marketplace for online services (indirect).[40] And certain state laws or constitutions may obligate private parties to provide fora for public expression.[41]

Still, enacted laws, such as those described above, represent only weak interventionism in favor of users or providers. State laws may be preempted by state constitutions or federal regulations, federal regulations by federal statutes, and even federal statutes can be repealed or modified with the next change of Congress.

Therefore, far more attractive to both users and providers is the prospect of strong interventionism in their favor. Users might prefer a federal constitutional right to access third-party platforms, and some have even argued that the First Amendment entitles them to speak their minds on Facebook or Twitter.[42] Providers, by contrast, have responded that the Constitution not only does not obligate them to host undesired user content but in fact *guarantees* them the right to exclude it, whether by virtue of their own First Amendment editorial rights or their Fifth Amendment freedom against uncompensated "takings" of their private property.[43] Thus, we see in Figure 1 that users' rights of access progress from laissez faire to weak interventionism to strong interventionism, depending on the particular laws invoked, while providers' rights to discriminate grow in the opposite direction.

With this taxonomy of positive law established, we now turn to theory. Regardless of what regulatory tools exist or could exist, how *should* the law function in this space? To aid in answering this question, I first survey the field of existing interventionist theories to evaluate their claims and to see if any one theory emerges that adequately balances the competing interests of users, providers, and society at large.

But first, a brief note about nomenclature. As stated, the two main characters in the drama that is content moderation are the user and the provider. These roles are defined not by anything intrinsic in the parties but by their relationship to each other. When an individual visits a website, she obviously does so as a user, while the website operator plays the role of provider. But that same website operator depends on services provided by vendors, such as ISPs, domain name system (DNS) intermediaries, and hosting companies and therefore should be regarded as a user in relation

---

40. *See* Mark A. Lemley, *The Contradictions of Platform Regulation*, 1 J. FREE SPEECH L. 303, 335 (2021) ("Effective antitrust enforcement that opens tech markets to competition may . . . [preserve] a choice of Internet platforms with . . . more content restrictions versus less . . . .").

41. *See infra* section I.C.1.

42. *See id.*

43. *See infra* section I.B.2, 4.

to those providers. Thus, even though the five internet rights primarily concern the resources on which website operators depend, I articulate them in terms of *user* rights, since they go to the issue of whether service providers should be able to prevent content from appearing on the internet by denying services to websites that would publish that content. Moreover, although I use the terms "provider" and "intermediary" interchangeably, "platform" has a narrower, more technical definition. As a subset of providers, platforms are best understood as entities that participate in two-sided markets, such as social media companies or ad networks.[44]

B. Provider-Centric Interventionism

We start with provider-centric theories, progressing from the laissez faire arena of deregulation to the weak interventionism of enacted statutes to the strong interventionism of constitutionally protected editorial rights.

1. Free Market

The Free Market theory might perhaps be better styled as a theory of *non*-interventionism. It posits that in the struggle for power between users and providers, the ideal balance is most likely to emerge when the government simply gets out of the way and allows the free market to work.[45]

Obviously, as between any one provider and any one user, this approach favors the provider, which remains free to accept or reject the user's content as it pleases. But that is not to concentrate all power in providers as a class. Rather, the Free Market theory takes a broader view, asserting that users, as a class, can discipline providers that operate with too heavy a hand or that unfairly discriminate against certain groups. For example, if an online forum earns a reputation for deleting only conservative comments, conservatives will presumably "vote with their feet," forcing the forum operator either to soften its position or reckon with the prospect of a smaller userbase. If all the major platforms show hostility toward far-left anarchist speech, that only presents a market

---

44. *See* Thomas B. Nachbar, *Platform Effects*, 62 JURIMETRICS 1, 8–9 (2021).

45. For recent examples of scholars and commentators who have embraced a Free Market theory of interventionism, see Lemley, *supra* note 40, at 324–27, 331–35; Ashutosh Bhagwat, *The Law of Facebook*, 54 U.C. DAVIS L. REV. 2353 (2021); ROBBY SOAVE, TECH PANIC: WHY WE SHOULDN'T FEAR FACEBOOK AND THE FUTURE (2021); Katherine Mangu-Ward, *Don't Try to Fix Big Tech with Politics*, REASON (July 2021), https://reason.com/2021/06/07/dont-try-to-fix-big-tech-with-politics/ [https://perma.cc/4MAT-Y22J]; Yoo, *supra* note 1, at 771.

opportunity for anarchist-friendly sites.[46] As former FCC Chairman Michael Powell argued in opposing net neutrality, "[d]egrading the internet, blocking speech and trampling what consumers now have come to expect"—the precise behavior prohibited by net neutrality rules—"would not be profitable, and the public backlash would be unbearable."[47] Government, therefore, doesn't need to intervene, because profit motives already incentivize major providers to cater to a diverse userbase and ensure that users with more niche viewpoints can find adequate alternatives.[48]

Even if the market fails to strike the optimum balance between users and providers, supporters of the Free Market theory have little faith that regulation could improve matters.[49] Governmental intervention is least likely to be effective in highly technical areas that are rapidly changing, a description that certainly matches the internet sector.[50] Although today's internet giants might seem unstoppable, the sheer dynamism of the online marketplace has toppled many leaders and replaced them with newly minted upstarts perhaps more quickly than any other industry.[51] Today's government regulations might badly miss the mark by targeting yesterday's villains or, worse, entrenching them.[52] Moreover, government

---

46. Tumblr, for example, saw its web traffic plummet by a third after it banned adult content, as porn-friendly copycat sites sprang up to capture disappointed users. *See* Sean Captain, *After Tumblr's NSFW Ban, These Adult Communities Have Come Out on Top*, FAST COMPANY (June 4, 2019), https://www.fastcompany.com/90358305/six-months-after-tumblrs-nsfw-ban-these-kink-communities-are-coming-out-on-top (last visited Apr. 30, 2023).

47. Michael Powell, *Let's Calm Down. No Matter What Happens with Net Neutrality, an Open Internet Isn't Going Anywhere*, VOX (Dec. 13, 2017, 6:15 AM), https://www.vox.com/2017/12/13/16768700/net-neutrality-vote-fcc-commissioner-ajit-pai-michael-powell-light-touch-regulation [https://perma.cc/CQU4-SC2J].

48. *See* Amanda Lotz, *Profit, Not Free Speech, Governs Media Companies' Decisions on Controversy*, CONVERSATION (Aug. 10, 2018, 6:41 AM), https://theconversation.com/profit-not-free-speech-governs-media-companies-decisions-on-controversy-101292 [https://perma.cc/M2Y4-HLTN].

49. *See* Lee, *supra* note 1, at 1034; Yoo, *supra* note 1, at 771 ("[A]ny attempt to regulate the manner in which these intermediaries sift through and present Internet content is likely to affect speech markets in ways that can be quite problematic.").

50. *See* William E. Kennard, Chairman, FCC, Remarks Before the National Cable Television Association: The Road Not Taken: Building a Broadband Future for America (June 15, 1999), http://www.fcc.gov/Speeches/Kennard/spwek921.html [https://perma.cc/B4FA-2RGF] ("[T]he best decision government ever made with respect to the Internet was the decision that the FCC made . . . NOT to impose regulation on it. . . . It was intentional restraint born of humility. Humility that we can't predict where this market is going.").

51. *See From Microsoft to Google to Facebook: The 20 Biggest Tech Companies that Dominate the Web (Infographic)*, DIGIT. INFO. WORLD, https://www.digitalinformationworld.com/2019/01/amazon-apple-yahoo-twitter-illustrating-20-internet-giants-since-1998.html [https://perma.cc/EC9A-EHM5].

52. *See* Lemley, *supra* note 40, at 326–27, 331.

regulation is typically a blunt tool, forcing a binary proposition of either leaving content up or taking it down. Far more promising is the prospect that industry players, left to themselves, can solve the tricky puzzle of problematic content through more nuanced software-based solutions, such as by de-amplifying outrageous content, contextualizing misleading information with labels or warnings, or simply inviting users to pause and think before they post a nasty remark.[53]

But the Free Market theory has its shortcomings. For one, it fails to account for the perverse incentives that stem from secondary liability. Under the common law, an intermediary may sometimes be held secondarily liable for content posted or distributed by its users, depending on whether the intermediary acted as a publisher or merely a distributor. As is well known in cyberlaw scholarship, the plaintiff in *Stratton Oakmont v. Prodigy*[54] won the right to pursue a $200 million verdict against Prodigy, an early ISP, after an anonymous subscriber posted defamatory content on a Prodigy bulletin board.[55] Central to the court's holding was the fact that Prodigy, unlike certain other ISPs, actively moderated content, which persuaded the court to classify Prodigy as a publisher and subject it to strict liability for all of its users' content.[56] The *Stratton Oakmont* case, therefore, signaled to online service providers that they were not, in fact, free to moderate user content as they saw fit. Instead, they were incentivized to forgo any content moderation at all, lest they be classified as publishers and held liable for their users' content.[57] To prevent this outcome, Congress enacted Section 230, which not only declared that online service providers should not be treated as publishers of their users' content but also expressly shielded providers from liability for that content, with minimal exceptions for intellectual property infringement, sex-trafficking, and other federal criminal laws.[58] Thus, if Section 230 is any guide, a free market for online content cannot thrive in a deregulated environment; it needs statutory intervention to allocate risks

53. *See* Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. REV. 1 (2021); Evelyn Mary Aswad, *The Future of Freedom of Expression Online*, 17 DUKE L. & TECH. REV. 26, 49–51 (2018).

54. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

55. *Id.* at *4; *see* Peter H. Lewis, *After Apology from Prodigy, Firm Drops Suit*, N.Y. TIMES (Oct. 25, 1995), https://www.nytimes.com/1995/10/25/business/after-apology-from-prodigy-firm-drops-suit.html [https://perma.cc/A9KG-B9BL] (noting that Stratton Oakmont sought $200 million in damages from Prodigy).

56. *Stratton Oakmont*, 1995 WL 323710, at *5.

57. KOSSEFF, *supra* note 8, at 56.

58. 47 U.S.C. §§ 230(c), (e).

and responsibilities between providers and users to be truly free.[59]

2. Provider Property Rights

Under the Provider Property Rights theory, the law should side with providers when it comes to content moderation not because it cares about the marketplace, or even about expression, but because providers should have the right to do as they please with their property.[60] Since providers own, or at least have exclusive possessory rights to, their hardware, software, and network cables, they should be able to exercise that most fundamental right within their property bundle of sticks: the right to exclude.[61]

As a matter of positive law, this theory finds its most well-known expression in the Computer Fraud and Abuse Act of 1986 (CFAA).[62] Enacted at a time when only 2,000 computers connected to the internet and webpages did not yet exist, the CFAA was intended to clarify what, at the time, was still an open question in the law: how should ancient doctrines of trespass, which assumed some kind of physical intrusion, apply to the mere sending of unsolicited electronic signals?[63] Initially, the CFAA started small, targeting only those who hacked into computer systems to steal valuable data or inflict economic damage.[64] Over time, however, the statute was amended to extend broadly to anyone who merely "exceeds authorized access . . . from any protected computer,"[65] which the Justice Department has used to prosecute users for simply violating a website's terms of service.[66] Similar prohibitions have been transposed to state law such that all fifty states now statutorily prohibit

---

59. *See id.* § 230(a)(2) (grounding provider protections in the need "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services").

60. For examples of scholars who have considered property rights as a basis for content moderation (positively or negatively), see authorities cited *supra* note 6.

61. *See* Mary Anne Franks, *Beyond the Public Square: Imagining Digital Democracy*, 131 YALE L.J. F. 427, 434 (2021) ("[T]he Supreme Court has long recognized that private-property owners generally have the right to exclude individuals from their property as they see fit."); Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730 (1998).

62. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified at 18 U.S.C. § 1030).

63. Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. 1184, 1194–95 (2022).

64. Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/WV96-B3AK]. Notably, the Supreme Court recently rejected (for the most part) the Justice Department's interpretation that merely violating a website's terms of service is actionable under the CFAA. *See* Van Buren v. United States, __ U.S. __, 141 S. Ct. 1648, 1660–62 (2021).

65. 18 U.S.C. § 1030(a)(2)(c).

66. Wu, *supra* note 64.

cybertrespass in one form or another.[67]

But the CFAA and its state analogs establish only a weak interventionist regime. Legislatures could repeal such laws or modify them to grant users the right to access providers' systems in some circumstances. Common carriage laws, as discussed further below,[68] do precisely that, requiring certain providers to accept all paying customers and preventing them from discriminating against lawful uses.[69]

As a result, some have entertained notions of a strong interventionist regime that would elevate providers' power to exclude to a constitutional right. Daniel Lyons, for example, has argued that the Obama administration's net neutrality rules, had they remained in place, would have effected a "permanent . . . occupation of private broadband networks and therefore take[n] broadband providers' property without just compensation."[70] Verizon later made the same argument in opposing the FCC's 2010 Open Internet Order.[71] Others have made similar arguments against laws that would regulate social media companies as common carriers by requiring them to host all lawful user content.[72] Or, even if such laws don't significantly burden a provider's property *per se*, they may nonetheless harm its economic interests.[73] Forced to host Holocaust denial videos, for example, YouTube might see its advertisers pull back and its userbase decline, all of which would hurt its bottom line.

The Constitution, however, erects a high bar before a Fifth Amendment taking will be found. In *Pruneyard Shopping Center v. Robins*,[74] the Supreme Court upheld an interpretation of the California Constitution requiring shopping centers to allow members of the public to distribute leaflets and gather signatures on their property.[75] California's rule clearly interferes with malls' right to exclude guests from their property, and it

---

67. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1597 (2003).

68. *See infra* section I.C.2.

69. Christopher S. Yoo, *Common Carriage's Domain*, 35 YALE J. ON REGUL. 991, 996 (2018) [hereinafter Yoo, *Common*].

70. Lyons, *supra* note 6, at 65.

71. *See* Brief for Petitioner-Appellant at 49–50, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355).

72. *E.g.*, Ilya Somin, *Why the Florida and Texas Social Media Laws Violate the Takings Clause*, REASON (Sept. 17, 2022, 4:43 PM), https://reason.com/volokh/2022/09/17/why-the-florida-and-texas-social-media-laws-violate-the-takings-clause/ [https://perma.cc/L8AG-XKQG]; Thierer, *supra* note 6, at 292–94; Berin Szóka & Corbin Barthold, *Justice Thomas's Misguided Concurrence on Platform Regulation*, LAWFARE (Apr. 14, 2021, 10:30 AM), https://www.lawfareblog.com/justice-thomass-misguided-concurrence-platform-regulation [https://perma.cc/LUJ4-KV3M].

73. *See* Volokh, *supra* note 2, at 435–37.

74. 447 U.S. 74 (1980).

75. *Id.* at 77–79.

may also hurt sales, since, as one scholar put it, "offended patrons are less likely to be in a shopping mood."[76] In fact, California's rule extends even to protesters who might surround a particular store within a mall to urge patrons to boycott it.[77] Yet the Court held that even this interference did not "unreasonably impair the value or use of [the appellant's] property as a shopping center" and therefore did not constitute a taking.[78] It would therefore be hard to argue that online service providers, which are likewise generally open to the public, would be any more burdened in their proprietary or economic interests by common carriage regulation, or at least burdened enough to support a claim under the Takings Clause.

But positive law aside, how do provider property rights hold up as a general theory of interventionism? Not so well, it seems.

First, the theory rests on a sort of property absolutism that has been rejected in other contexts. Regulations routinely burden firms to advance other important interests, such as protecting the environment or ensuring a level playing field. To assert that online service providers should enjoy total freedom from the economic burdens of content-related regulation or from general requirements to serve users is to adopt a Lochnerian view of property rights that finds little support in the modern regulatory state. It has also fared poorly as a weapon against anti-discrimination laws that burden citizens' rights to use their property as they see fit.[79] In sum, "my property, my rules" may still hold water in intimate or personal settings, but it is hardly a trump card when it comes to participating in the modern economy.

Second, and related to the first, the theory fails to adequately account for user interests for the simple reason that users, typically, have no property interests of their own. It is common today to speak of the "digital divide," which refers to the distinction between those groups or regions that have access to modern information and communications technology and those that do not.[80] Less remarked upon is what might be called the *digital property divide*. Although users often own the devices they use to communicate online—their laptops and smartphones, for instance—few possess the network infrastructure to disseminate their opinions beyond their homes. Instead, they must rely on ISPs to connect to the internet,

---

76. Volokh, *supra* note 2, at 435.

77. *Id.*

78. *Pruneyard Shopping Ctr.*, 447 U.S. at 83.

79. *See, e.g.*, David v. Vesta Co., 45 N.J. 301, 311 (N.J. Sup. Ct. 1965) (rejecting a constitutional challenge to New Jersey's non-discriminatory housing laws, in which landowners argued that "one person has as much of a right to dispose of his real property as does another person to acquire it"); *id.* at 311 ("Private property rights are not absolute.").

80. *See* JAN VAN DIJK, THE DIGITAL DIVIDE 1 (2020).

email providers to send and receive communications, social media platforms to publish videos, and countless other providers ancillary to those functions. Given that cyberspace lacks the equivalent of public streets, parks, and sidewalks,[81] the result is that the vast population of unpropertied users can speak only at the pleasure of a small collection of propertied companies, a situation that should perhaps be just as concerning in the online context as it would be in the offline context.[82]

3. Good Samaritanism

According to the theory of Good Samaritanism, providers play a crucial role in cleaning up the internet; the law should therefore intervene where necessary to remove impediments to their doing so.[83]

For example, TikTok, a social media platform that caters to a younger demographic, prohibits users from posting sexually explicit content[84] and employs artificial intelligence to automatically detect and block nude imagery and other content unsuitable for minors.[85] Google reserves the right to ban shopping ads "that display shocking content or promote hatred, intolerance, discrimination, or violence."[86] And many online fora empower moderators to prevent bullying or abusive language.[87] Such measures enable providers to offer safe or family-friendly environments to users who want them.

But, as described above, the *Stratton Oakmont* decision threatened to tie providers' hands in that regard.[88] By classifying as publishers those companies that actively moderated their users' content, the case presented

---

81. *See* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1117 (2005).

82. *See* Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 533 (2003) ("Public spaces sometimes provide a subsidy to the poor: anyone can enter a city park, while a private garden would exist only if it could charge enough to be self-supporting.").

83. For examples of scholars who have embraced this viewpoint, see sources cited *supra* note 8.

84. *Community Guidelines*, TIKTOK, https://www.tiktok.com/community-guidelines [https://perma.cc/LTH8-LMKK] (last updated Oct. 2022).

85. Amy Iverson, *TikTok's New Software Automatically Removes Nudity. Why Don't All Social Media Networks Do This?*, DESERET NEWS (July 27, 2021), https://www.deseret.com/2021/7/27/22575979/tiktoks-new-software-automatically-removes-nudity-why-dont-all-social-media-networks-do-this [https://perma.cc/N368-3UAV].

86. *Google Merchant Center: Shopping Ads Policies*, GOOGLE HELP, https://support.google.com/merchants/answer/6149970?hl=en&rd=1#US [https://perma.cc/8RT3-A2CY].

87. *Moderators: The Quiet Community Protectors*, MODSQUAD (Feb. 25, 2020), https://blog.modsquad.com/blog/moderators-the-quiet-community-protectors/ ("Most online communities have forms and reports where users can flag problematic content for review, including instances of bullying.") [https://perma.cc/6L5H-QPHB].

88. *See supra* section I.B.1.

providers with three equally unpalatable options: moderate perfectly (and assume the operational costs of reviewing every bit of user content), moderate imperfectly (and assume the risk of secondary liability for any problematic content missed), or abstain from moderation altogether (and allow bad users to spoil the party for other users). Section 230(c)(1) removed this trilemma by declaring that online providers should not be regarded as publishers of their users' content.[89]

Had Section 230 stopped at that point, it might only support a free market ethic. It would have prevented pesky third parties from using an anachronistic common law doctrine to choke the growth of the internet but otherwise refrained from placing a thumb on the scale between providers and their users. But legislators *did* wish to place a thumb on the scale. Titled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material," Section 230(c) went on to shield online providers from liability for actions "taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[90] And it preempted any inconsistent state laws that might hold service providers liable for such moderation decisions.[91]

As Jeff Kosseff chronicles, the bill that became Section 230 grew out of a broader moral panic surrounding the sudden ubiquity of online pornography and the ease with which children could access it.[92] Contrasted with other provisions in the Communications Decency Act that effectively *required* providers to block access to "indecent" content in certain contexts (a forced takedown regime),[93] Section 230 took a lighter approach by simply removing barriers for providers to voluntarily do so. But the goal was the same: to encourage providers to act as "good Samaritans" by taking down offensive content that the First Amendment prevented the government from targeting directly.[94]

---

89. 47 U.S.C. § 230(c)(1).

90. *Id.* § 230(c)(2).

91. *Id.* § 230(e)(3).

92. KOSSEFF, *supra* note 8, at 61–76.

93. 47 U.S.C. §§ 223(a), (b)(3).

94. *See* Jane Bambauer, James Rollins & Vincent Yesue, *Platforms: The First Amendment's Misfits*, 97 IND. L.J. 1047, 1048 (2022) ("[T]he dominant conception of Section 230 actually *encourages* platforms to do this sort of purging in order to help internet users avoid the toxic effects of illegal or lawful-but-awful content." (emphasis in original)); Nunziato, *supra* note 81, at 1129; Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR (Mar. 21, 2018, 5:11 AM), https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change [https://perma.cc/E2BL-6AGS] ("The original purpose of [Section 230] was to help clean up the Internet." (quoting Congressman Christopher Cox)).

Few, I think, would argue with the proposition that providers play an important role in removing content that detracts from the online experiences we desire. But does the law need to intervene to give providers that power? And does Section 230, the archetype of Good Samaritanism, strike the right balance between provider and user interests? Some don't think so. As for the original goal of protecting the nascent commercial internet from rampant defamation suits, it's far from certain that secondary liability posed a meaningful threat. As Brent Skorup and Jennifer Huddleston have detailed, courts had already been narrowing publisher liability for decades before the internet emerged.[95] Section 230, therefore, may have only slightly accelerated what was already a secular trend toward protecting providers from liability for user-generated content. Thus, the common law might have already sufficed to shield providers from crushing secondary liability, notwithstanding the contrary result in what was then only a single, potentially aberrant, state trial court decision in *Stratton Oakmont*.

Moreover, Good Samaritanism can itself foster bad behavior where it is not accompanied by appropriate limiting principles. As Danielle Citron and Benjamin Wittes have shown, by exempting providers from liability even for bad user content they know about or encourage, Section 230 provides a regulatory shield for "Bad Samaritans" to operate websites that deliberately cater to toxic or even illegal content, such as revenge porn, doxing, or sexual grooming.[96] Conversely, Good Samaritanism, left unchecked, would seemingly allow any online provider to dictate what content should be allowed on the internet, so far as it can control distribution, no matter how deep the provider operates within the internet or how far removed from user expression it operates.[97] Such deep deplatforming threatens the underlying neutrality of the internet itself and is at odds with other regulatory interventions, such as net neutrality.[98]

In sum, statutory intervention may not be necessary for Good Samaritan providers to clean up the internet and in fact may either hinder that goal or take it too far.

---

95. *See* Brent Skorup & Jennifer Huddleston, *The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation*, 72 OKLA. L. REV. 635, 637–48 (2020).

96. *See generally* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401 (2017).

97. *See infra* section II.A.

98. *See* Aswad, *supra* note 53, at 55 (criticizing a conception of "good corporate citizenship" that focuses predominantly on "ban[ning] speech" and suggesting an alternative conception that "respect[s] international human rights standards when curating content").

4. Editorial Rights

Still, the most popular argument in favor of allowing providers to moderate content as they please is that the First Amendment protects their editorial right to do so.[99] In fact, to call the Editorial Rights theory popular may not even do it justice. It is almost taken as an article of faith that the First Amendment protects online providers' right to take down undesired content and that "it's not a close question."[100]

Support for the Editorial Rights theory starts with *Miami Herald Publishing Co. v. Tornillo*,[101] in which the Supreme Court unanimously struck down a Florida law requiring newspapers to print responses from political candidates who were criticized in their newspapers.[102] Noting that a newspaper is more than a "passive receptacle or conduit for news, comment, and advertising," the Court explained that the choice of what "material [should] go into a newspaper . . . and [the] treatment of public issues and officials . . . constitute the exercise of editorial control and judgment."[103] Interfering with that judgment violated the First Amendment's guarantee of a free press.[104] Nor could it be said that newspapers retained their editorial judgment by virtue of the fact that the right-of-reply statute required them merely to append a small amount additional material. Because newspapers must fit all their material into a limited physical format, printing mandatory rebuttals would "tak[e] up space that could be devoted to other material the newspaper may have preferred to print."[105]

Later cases expanded the concept of editorial rights beyond the traditional press. In *Hurley v. Irish-American Gay, Lesbian & Bisexual Group of Boston*,[106] for example, the Court held that private organizers could not be compelled to include floats or messages in a public parade that they disapproved of because doing so would alter the overall message the organizers wished to convey.[107] Together, these and other cases stand

99. For examples of scholars who appear to hold this position, at least as to certain types of providers, see Bhagwat, *supra* note 1; Lee, *supra* note 1, at 1035; John Blevins, *The New Scarcity: A First Amendment Framework for Regulating Access to Digital Media Platforms*, 79 TENN. L. REV. 353, 398–401 (2012) (as to search engines and social networks); Yoo, *supra* note 1, at 771–73; Chandler, *supra* note 1, at 1124–29.

100. Goldman, *supra* note 1.

101. 418 U.S. 241 (1974).

102. *Id.* at 256–58.

103. *Id.*

104. *Id.*

105. *Id.* at 256.

106. 515 U.S. 557 (1995).

107. *Id.* at 572–73.

for the proposition that even if a medium distributes only third-party content, the operator of that medium may nonetheless be considered a speaker as to such content if, by choosing which items to include or exclude, the operator creates a "coherent speech product" that conveys an overall message.[108]

In the same manner, those who subscribe to the strong interventionism of the Editorial Rights theory argue that online providers exercise editorial judgment in deciding which user content to allow or disallow.[109] Likewise, providers' content policies may convey overall messages, such as gender equality or pro-life values, depending on the provider.[110] Thus, laws that require online providers to carry all lawful user speech would interfere with providers' editorial rights and alter the overall messages they wish to convey.

While it's certainly possible that the Supreme Court will eventually expand the editorial rights doctrine of *Miami Herald*, *Hurley*, and other cases to certain online providers, as Eugene Volokh has shown, none of these cases clearly compels that result.[111] Contrary to popular belief, whether social media companies could be treated as common carriers remains an open question.[112] Unlike the newspapers at issue in *Miami Herald*, social media companies do not make *ex ante* individualized decisions about which user posts should be published but instead operate far more like "passive receptacle[s] . . . for news [and] comment."[113] Many websites, such as social media platforms, also do not operate with the same space constraints. As essentially limitless fora for user speech, such websites can easily host additional user posts without dropping other posts to make everything fit. Unlike newspapers, banners, or parades, many online service providers do not put out anything approximating a coherent speech product, since domain registries, video catalogs, and the

108. Volokh, *supra* note 2, at 423–25.

109. *See* Goldman, *supra* note 1.

110. *See* Volokh, *supra* note 2, at 405 n.106.

111. *See id.* at 415–28 (arguing that compelling social media companies to host all lawful user content would be constitutional, provided that such companies are not compelled to speak or restricted from speaking and user content is not likely to be attributed to the companies) (first citing Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74 (1979); then citing Rumsfeld v. F. for Acad. & Institutional Rts., Inc., 547 U.S. 47 (2006); and then citing Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180 (1997)).

112. *Compare* NetChoice, LLC v. AG, Fla., 34 F.4th 1196, 1221–22 (11th Cir. 2022) (rejecting Florida's attempt to regulate social media companies as common carriers under the First Amendment), *with* Netchoice, LLC v. Paxton, 49 F.4th 439, 473 (5th Cir. 2022) (upholding Texas's regulation of social media companies as common carriers against a First Amendment challenge).

113. Miami Herald Pub. Co. v. Tornillo, 418 U.S. 241, 258 (1974).

universe of tweets can hardly be digested by any one user.[114] And while online providers can tailor their content policies to create certain online experiences for other users (e.g., an LGBT-friendly site), under *Pruneyard*, a shopping center's desire to provide a generically appealing environment for patrons (e.g., family-friendly) is not sufficiently concrete to constitute an overall message for First Amendment purposes.[115] Perhaps summarizing it best, Justice Breyer noted, "[r]equiring someone to host another person's speech is often a perfectly legitimate thing for the Government to do."[116]

But case law aside, the Editorial Rights theory presents a deeper philosophical problem. If merely propagating user content and having the ability to block or take down that content based on a provider's terms of service amounts to constitutionally protected provider speech, then what *isn't* provider speech? Inasmuch as nearly everything on the internet is connected in some way with transmitting or facilitating speech, an overly expansive view of the First Amendment threatens to erect a regulatory shield over most internet functions,[117] a position that is at odds with the long history of telecommunications regulation in the United States.[118] As if to underscore the point, in *Verizon v. FCC*,[119] various ISPs argued that the FCC's net neutrality regulations abridged their First Amendment rights because such rules had the effect of "stripping them of control over the transmission of speech on their networks,"[120] a position later echoed

114. As further explained in section III.B.3, a domain registry for a given top-level domain (e.g., .com, .org, and .edu) is an authoritative database that indicates which entity has registered each domain name in the top-level domain. *See also* Nicholas Nugent, *Masters of Their Own Domains: Property Rights as a Bulwark Against DNS Censorship*, 19 COLO. TECH. L.J. 43, 56–64 (2021).

115. *See* Ctr. for Bio-Ethical Reform, Inc. v. Irvine Co., 249 Cal. Rptr. 3d 391, 399–400 (Cal. Ct. App. 2019) (rejecting a shopping center's claim that requiring it to permit anti-abortion activists to display grisly depictions of abortion violated its First Amendment rights to create a "family-oriented" environment).

116. Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 591 U.S. __, 140 S. Ct. 2082, 2098 (2020) (Breyer, J., dissenting).

117. *See* Alan Z. Rozenshtein, *Silicon Valley's Speech: Technology Giants and the Deregulatory First Amendment*, 1 J. FREE SPEECH L. 337, 347–56 (2021) (describing "regulatory battlegrounds for Silicon Valley's free-expression arguments" against various forms of regulation or government actions); Mary Anne Franks, *The Free Speech Black Hole: Can the Internet Escape the Gravitational Pull of the First Amendment?*, *in* FREE SPEECH FUTURES, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Aug. 21, 2019), https://knightcolumbia.org/content/the-free-speech-black-hole-can-the-internet-escape-the-gravitational-pull-of-the-first-amendment [https://perma.cc/QB4W-6R4T]; *cf.* Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133 (2016); Leslie Kendrick, *First Amendment Expansionism*, 56 WM. & MARY L. REV. 1199 (2015).

118. *See* Susan Crawford, *First Amendment Common Sense*, 127 HARV. L. REV. 2342 (2014).

119. 740 F.3d 623 (2014).

120. Brief for Petitioner-Appellant, *supra* note 71, at 3.

by then-Judge Kavanaugh.[121] Yet, if ISPs, which merely act as passive conduits for internet traffic, have constitutionally protected editorial rights to block whichever communications they dislike, it is hard to see why traditional telephone companies, which have long been regulated as common carriers, could not make the same argument.

In sum, while the First Amendment may ultimately be found to protect the content moderation practices of certain online providers, such as social media platforms and other web-based fora (or not), it seems plain that editorial rights do not provide a workable theory of interventionism more broadly.

C. User-Centric Interventionism

Unlike provider-centric interventionism, which boasts the CFAA and Section 230, user-centric interventionism lacks any federal laws that explicitly entitle users to access private online services. But that has not stopped scholars and litigants from arguing that existing laws already implicitly grant such rights, nor has it stopped legislators from proposing new laws to shift some power back to users when it comes to content moderation. In this section, I analyze three user-centric theories that animate these efforts, starting with the strong interventionism of constitutionally protected user expressive rights and moving to weak interventionist theories based on non-discrimination and property rights.

1. Expressive Rights

When it comes to user-centric interventionism, the most obvious user interest advanced by forced carriage regulation is user expression. Many users simply wish to express themselves online without interference by private providers. Few would disagree that robust online discourse yields many societal benefits, and many believe that openly discussing heterodox, or even offensive, viewpoints is essential to maximizing these benefits.[122] But does it follow that the state should legally protect the right

---

121. U.S. Telecomms. Ass'n v. FCC, 855 F.3d 381, 418 (2017) (Kavanaugh, J., dissenting from denial of rehearing en banc) ("[T]he First Amendment bars the Government from restricting the editorial discretion of Internet service providers, absent a showing that an Internet service provider possesses market power in a relevant geographic market.").

122. *See* Martha McCaughney, *Putting Out the Fire: Common Reading Programs as Flash Points in Campus Culture Wars*, AM. ASS'N OF COLLS. & UNIVS. (2021), https://www.aacu.org/liberaleducation/articles/putting-out-the-fire [https://perma.cc/UU2W-T72Q] ("Students must be taught that the university, as a place of polyvocality, will expose them to new—and sometimes even shocking or offensive—ideas that might challenge their beliefs and personal identities."); GREG LUKIANOFF & JONATHAN HAIDT, THE CODDLING OF THE AMERICAN MIND: HOW GOOD INTENTIONS AND BAD IDEAS ARE SETTING UP A GENERATION FOR FAILURE (2018).

of unpopular users to speak their minds in certain online venues? Some think so, arguing that the law should protect political discourse from the "unparalleled power" of private technology platforms by preventing them from "censor[ing] speech based on its political content."[123]

The strong form of this argument posits that the First Amendment protects users' speech in cyberspace just as surely as it does in real space, not only from government interference but also from private providers that seek to "censor" them.[124] Because the First Amendment generally applies only to the state,[125] arguments for treating certain online service providers as state actors have proliferated in recent years, many of them focused on social media companies.[126] But state action arguments about private internet actors predate the rise of social media, going back as far as the late 1990s and early 2000s.[127] In fact, until the mid-2010s, when the political right began grumbling that conservative viewpoints were being targeted by Big Tech, one might say that such state action arguments were even fashionable among left-leaning academics while being eschewed by

123. Prasad Krishnamurthy & Erwin Chemerinsky, *How Congress Can Prevent Big Tech from Becoming the Speech Police*, HILL (Feb. 18, 2021, 8:00 AM), https://thehill.com/opinion/judiciary/539341-how-congress-can-prevent-big-tech-from-becoming-the-speech-police/ [https://perma.cc/3845-MFBY]; *see also* Volokh, *supra* note 2, at 392 ("I'm inclined to agree."); Laura Stein, *Speech Without Rights: The Status of Public Space on the Internet*, 11 COMMC'N REV. 1, 18–19 (2008).

124. For examples of scholars and commentators who appear to have entertained some version this thesis at some point, see Ramaswamy & Rubenfeld, *supra* note 9; Tim Wu, *Is the First Amendment Obsolete?*, 117 MICH. L. REV. 547, 577–78 (2018); Langvardt, *supra* note 5, at 1366; Eric Sirota, *Can the First Amendment Save Net Neutrality?*, 70 BAYLOR L. REV. 781 (2018); Mason C. Shefa, *First Amendment 2.0: Revisiting* Marsh *and the Quasi-Public Forum in the Age of Social Media*, 41 U. HAW. L. REV. 159, 184–87 (2018); Jonathan Peters, *The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application—or Lack Thereof—to Third-Party Platforms*, 32 BERKELEY TECH. L.J. 989, 1022–24 (2017); DAWN NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 134–51 (2009).

125. Manhattan Cmty. Access Corp. v. Halleck, 587 U.S. __, 139 S. Ct. 1921, 1928 (2019).

126. *See, e.g.*, Ramaswamy & Rubenfeld, *supra* note 9 ("Google, Facebook and Twitter should be treated as state actors under existing legal doctrines"); Victoria Baranetsky, *Keeping the New Governors Accountable: Expanding the First Amendment Right of Access to Silicon Valley*, KNIGHT FIRST AMEND. INST. (Aug. 21, 2019), https://knightcolumbia.org/content/keeping-the-new-governors-accountable-expanding-the-first-amendment-right-of-access-to-silicon-valley [https://perma.cc/7ZG8-HKQJ] ("[E]xpanding the state action doctrine to [social media] companies would align with the First Amendment's right of the listeners."); Shefa, *supra* note 124, at 187 ("[A]lthough Nextdoor might not be a quasi-public forum, it arguably still may qualify as a state actor which may not violate its users' First Amendment rights.").

127. *See, e.g.*, A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 117–25 (2000) (arguing that ICANN is a state actor); Jonathan Zittrain, *ICANN: Between the Public and the Private*, 14 BERKELEY TECH. L.J. 1071, 1092 (1999) ("ICANN is fashioned as a private, public interest municipal government."); Cyber Promotions v. Am. Online, 948 F. Supp. 436, 437–39 (E.D. Pa. 1996) (adjudicating a spammer's claim that it had a First Amendment right not to have its emails blocked by a private email service provider).

the right, commitments that have now reversed themselves.

Most state action arguments center on the public function doctrine, which holds that a private party may be regarded as a state actor when it performs a function traditionally performed by the state.[128] In *Marsh v. Alabama*,[129] which inaugurated the doctrine, the Supreme Court upheld the First Amendment rights of a Jehovah's Witness to distribute religious literature on the streets of a privately owned company town, reasoning that "[t]he more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it."[130] Some have pointed to this language to argue that intermediaries that operate certain online services that are generally open to the public should no more be able censor constitutionally protected speech than could the Gulf Shipbuilding Corporation in Chickasaw, Alabama.[131]

But after reaching its zenith in *Amalgamated Food Employees Union v. Logan Valley Plaza*,[132] which recognized a First Amendment right to protest in private shopping malls,[133] the Court walked back from *Marsh's* broad statement, holding that public functions are limited to those performed traditionally,[134] and later *exclusively*,[135] by the state. While it could be said that certain internet functions were traditionally performed by the state—after all, the internet was born out of the government-sponsored ARPANET and NSFNET research projects, and the Commerce Department ran the early domain name system through its contracts with Network Solutions—none of these functions is now performed *exclusively* by the state. On the contrary, ever since the Commerce Department relinquished its control over ICANN in 2016,[136] every modern internet function has been performed almost exclusively by *private* entities. Nor

128. Marsh v. Alabama, 326 U.S. 501, 506 (1946).

129. 326 U.S. 501 (1946).

130. *Id.* at 506.

131. *See, e.g.*, Brief for Petitioner-Appellant at 36–55, Prager Univ. v. Google LLC & YouTube, 951 F.3d 991 (9th Cir. 2020) (No. 18-15712) (arguing that YouTube qualifies as a state actor under *Marsh* and its progeny).

132. 391 U.S. 308 (1968).

133. *Id.* at 325.

134. Hudgens v. NLRB, 424 U.S. 507, 519–21 (1976).

135. S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm., 483 U.S. 522, 545 (1987).

136. *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/9648-TRAM] ("This historic moment marks the transition of the coordination and management of the Internet's unique identifiers to the private-sector, a process that has been committed to and underway since 1998.").

do other state action doctrines that have emerged since *Marsh*, such as "symbiosis" or "entanglement," provide a stronger basis for treating any broad class of online service providers as state actors.[137]

To be sure, courts have at times teased interventionists with dicta suggesting that the law may soon change. Most notably, in *Packingham v. North Carolina*,[138] Justice Kennedy, writing for the majority, paid homage to the "fundamental principle of the First Amendment" that "all persons have access to places where they can speak and listen."[139] He then referred to cyberspace as "the most important place[] . . . for the exchange of views" and to social media as "the modern public square."[140] Several commentators have therefore seized on this language to argue that the Court has recognized, or will soon recognize, social media as a "public forum" subject to First Amendment constraints.[141]

But these hopes are misplaced. *Packingham* concerned a North Carolina law that prohibited convicted sex offenders from accessing social media.[142] The issue was therefore whether the *state* could bar access to such important fora for public discourse, not whether social media providers themselves could bar particular users. And it is instructive that in multiple cases in which users have asserted First Amendment claims against private online service providers, some of which have cited *Packingham*, not a single litigant has prevailed.[143]

Even if the Constitution doesn't compel providers to extend free speech rights to their users, perhaps creating such rights by statute would nevertheless be good policy. As Genevieve Lakier has chronicled, various state laws, and some state constitutions, provide citizens with greater expressive rights than does the First Amendment.[144] For example, as

---

137. *See e.g.*, Alan Z. Rozenshtein, *No, Facebook and Google Are Not State Actors*, LAWFARE (Nov. 12, 2019, 8:30 AM), https://www.lawfareblog.com/no-facebook-and-google-are-not-state-actors [https://perma.cc/J4BP-5LTT] (critiquing Jed Rubenfeld's arguments that Section 230 essentially conscripts private website operators to censor user speech that the state could not constitutionally reach).

138. 582 U.S. __, 137 S. Ct. 1730 (2017).

139. *Id.* at 1735.

140. *Id.* at 1735, 1737.

141. *E.g.*, Baranetsky, *supra* note 126.

142. *Packingham*, 137 S. Ct. at 1733.

143. *See, e.g.*, Freedom Watch, Inc. v. Google, Inc., 368 F. Supp. 3d 30, 40–41 (D.D.C. 2019) (rejecting the plaintiff's reliance on *Packingham* to assert a constitutional right against private content moderation), *aff'd* 816 Fed. Appx. 497 (D.C. Cir. 2020); Atkinson v. Facebook Inc., No. 20-cv-05546-RS, 2020 U.S. Dist. LEXIS 263319, at *6–8 (N.D. Cal. Dec. 7, 2020) (same); Prager Univ. v. Google LLC, No. 17-CV-06064, 2018 U.S. Dist. LEXIS 51000, at *24–25 (N.D. Cal. Mar. 26, 2018) (same).

144. *See* Genevieve Lakier, *The Non–First Amendment Law of Freedom of Speech*, 134 HARV. L. REV. 2299, 2301–02, 2306–42 (2021).

described in connection with the *Pruneyard* case, California's state constitution guarantees citizens the right to protest in private shopping malls.[145] New Jersey's supreme court has likewise interpreted its state constitution to grant members of the public certain rights of expression and assembly on private university grounds.[146] As a matter of weak interventionism, should state or federal legislators extend similar expressive rights to those who wish to protest in virtual shopping malls or other online spaces?

The answer, I think, depends on the degree to which First Amendment principles are applicable to the private sector and to cyberspace in particular. Philosophical justifications for free speech include the search for truth and the centrality of free speech to self-government.[147] The question is whether these reasons for protecting citizen speech from government interference also merit protecting online user speech from private interference.

The search for truth justification—most famously captured in Justice Holmes's "marketplace of ideas" metaphor—asserts that the "truth is most likely to emerge when all opinions are expressed openly,"[148] a dynamic that is obviously absent if a single powerful entity can prevent others from expressing ideas it dislikes. Extending this reasoning to cyberspace, it could be argued that if most public discourse today occurs on social media platforms, and if those platforms do not allow users to express themselves freely, then the search for truth will be hindered, even though those arbiters of truth are private entities.[149] For example, during the heart of the COVID-19 pandemic, Facebook, Twitter, Reddit, and other large social media companies clamped down on the claim that the novel coronavirus originally leaked from a Wuhan lab or was in any way engineered (the "lab leak theory"), banning and suspending users who advanced the claim for trafficking in misinformation and conspiracy

145. Robins v. Pruneyard Shopping Ctr., 592 P.2d 341, 347 (Cal. 1979).

146. *See* State v. Schmid, 423 A.2d 615, 633 (N.J. 1980).

147. *See* FREDERICK SCHAUER, FREE SPEECH: A PHILOSOPHICAL ENQUIRY (1982) (cataloging popular theories of free speech).

148. Lawrence B. Solum, *Freedom of Communicative Action: A Theory of the First Amendment Freedom of Speech*, 83 NW. U. L. REV. 54, 68–69 (1989). For completeness, the four traditional rationales for free speech are the search for truth, self-government, autonomy, and self-realization. *Id.* at 68. However, because I regard the search for truth and self-government rationales as most applicable to the Expressive Rights theory I articulate in this section, I have omitted discussion of the autonomy and self-realization rationales. *See generally* Vincent Blasi, *Holmes and the Marketplace of Ideas*, 2004 SUP. CT. REV. 1, 4 (2004).

149. *See* Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media*, 1 J. FREE SPEECH L. 71, 78 (2021).

theory.[150] After the scientific community embraced the lab leak theory as a respectable conjecture, social media companies were forced to revise their policies, which has led many to wonder whether such companies may be harming the search for truth by suppressing other viewpoints that, while unpopular now, might later be vindicated.[151]

Free speech has also been justified as an essential element for democracy. As Lawrence Solum put it, for citizens to participate in the process of self-government, they must both "have access to information relevant to their decisions" and be able to freely "communicate their desires and opinions."[152] While, again, public censorship presents the greatest threat to self-government, private online firms, if large and powerful enough, can also distort the democratic process. For example, in the run-up to the 2020 presidential election, Facebook, Twitter, and other social media providers prevented users from sharing a *New York Post* article critical of then-candidate Joe Biden based on information discovered on a laptop abandoned by Hunter Biden.[153] Major social media providers have also directly suppressed or shaped statements made by elected officials on their platforms, from displaying critical notices next to debatable claims[154] to suspending officials' accounts until they agree to remove posts that express certain ideologies[155] to, most famously, banning

150. *See, e.g.*, Guy Rosen, *An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19*, META (Feb. 8, 2021), https://about.fb.com/news/2020/04/covid-19-misinfo-update/#removing-more-false-claims [https://perma.cc/T6JV-SEHA] (announcing enforcement actions against "false claims" that "COVID-19 is man-made or manufactured"); Rowan Jacobsen, *How Amateur Sleuths Broke the Wuhan Lab Story and Embarrassed the Media*, NEWSWEEK (Jan. 2, 2021, 2:23 PM), https://www.newsweek.com/exclusive-how-amateur-sleuths-broke-wuhan-lab-story-embarrassed-media-1596958 [https://perma.cc/5SZW-8B54] (reporting the immediate suspension of the Reddit account of an amateur sleuth after he posted another's theory about the origin of the COVID-19 virus).

151. *See* Robby Soave, *The Media's Lab Leak Debacle Shows Why Banning 'Misinformation' Is a Terrible Idea*, REASON (June 4, 2021, 7:30 AM), https://reason.com/2021/06/04/lab-leak-misinformation-media-fauci-covid-19/ [https://perma.cc/JY8R-XZRR].

152. Solum, *supra* note 148, at 73; *id.* at 72 n.68 (conceptualizing the importance of speech through the metaphor of a town meeting).

153. Kari Paul, *Facebook and Twitter Restrict Controversial New York Post Story on Joe Biden*, GUARDIAN (Oct. 14, 2020), https://www.theguardian.com/technology/2020/oct/14/facebook-twitter-new-york-post-hunter-biden [https://perma.cc/8PF8-N9Q8].

154. Donie O'Sullivan & Marshall Cohen, *Facebook Begins Labeling, but Not Fact-Checking, Posts from Trump and Biden*, CNN BUS. (July 21, 2020, 2:34 PM), https://www.cnn.com/2020/07/21/tech/facebook-label-trump-biden/index.html [https://perma.cc/NR5T-ZFSP].

155. *See* Kyle Morris, *Facebook Censored Blackburn Post After She Claimed 'Biological Men Have No Place' in Female Sports*, FOX NEWS (May 20, 2022, 1:23 PM), https://www.foxnews.com/politics/facebook-censored-blackburn-post-biological-men-womens-sports [https://perma.cc/D2H8-3SWQ].

then-President Trump from their platforms.[156] To be sure, in taking such actions, platforms claim to be neutrally applying their terms of service rather than acting out of ideological bias, which may be true.[157] But that platforms used by more than half of all Americans,[158] many of which get their news primarily from social media,[159] have the *power* to manipulate political discourse and potentially even sway elections through their content moderation decisions is, to some, reason enough to regulate that power.[160]

These arguments have merit, certainly, but they don't *compel* the conclusion that the state should extend free speech rights to users on private online platforms. While it's fair to say that the major social media players hindered the search for truth when it came to the lab leak theory, that impediment ultimately proved rather minor. Discussion continued elsewhere on the internet—through blogs, niche media sites, and the like—until support for the theory reached critical mass elsewhere and social media was forced to reverse course.[161] All told, the lab leak theory was banned on Facebook a mere three and a half months[162]—hardly a Galilean persecution. And while the marketplace of ideas metaphor makes intuitive sense for society as a whole, it's far from clear that "more speech" is the cure for bad speech on *individual* websites.[163] As Zeynep Tufecki and others have chronicled, trolls and other bad actors have become especially adept at harnessing mass communication platforms,

---

156. *Twitter 'Permanently Suspends' Trump's Account*, BBC NEWS (Jan. 9, 2021), https://www.bbc.com/news/world-us-canada-55597840 [https://perma.cc/9M97-39Y9].

157. In the case of the Hunter Biden laptop story, for instance, Twitter claimed to have blocked the story because of a policy against promulgating news based on illegally obtained information, whereas Facebook claimed that it needed time to determine if the story was false. *See* Adi Robertson, *Facebook and Twitter Are Restricting a Disputed New York Post Story About Joe Biden's Son*, VERGE (Oct. 14, 2020, 9:19 AM), https://www.theverge.com/2020/10/14/21515972/facebook-new-york-post-hunter-biden-story-fact-checking-reduced-distribution-election-misinformation [https://perma.cc/3W9L-6BFW].

158. *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/HA5J-UNNM].

159. Peter Suciu, *More Americans Are Getting Their News from Social Media*, FORBES (Oct. 11, 2019, 10:35 AM), https://www.forbes.com/sites/petersuciu/2019/10/11/more-americans-are-getting-their-news-from-social-media/?sh=1aecc9803e17 [https://perma.cc/4XVF-9V85].

160. *See, e.g.*, Volokh, *supra* note 2, at 388–95 (likening conservative discomfort with the power of large technology companies over speech to progressives' concerns about the political power of massive corporations).

161. Jacobsen, *supra* note 150.

162. *See* Rosen, *supra* note 150.

163. *See* Jonathan Zittrain, *The Inexorable Push for Infrastructure Moderation*, TECHDIRT (Sept. 24, 2021, 12:09 PM), https://www.techdirt.com/2021/09/24/inexorable-push-infrastructure-moderation/ [https://perma.cc/4986-EL9W] ("[I]t's difficult to say that the marketplace of ideas is outing only the most compelling ones.").

such as social media, to drown out healthy speech[164] and even to drive away certain voices altogether.[165]

And even if critics are rightly concerned that social media companies have too much power over the democratic process, it isn't clear that limiting their discretion to moderate content would produce a better result. Powerful social media tools coupled with lax rule enforcement can be just as detrimental to democracy if disinformation runs rampant and sophisticated users can "flood the zone with shit."[166] In fact, given that the U.S. presidential election was only days away, one could argue it was prudent to take care that the Hunter Biden laptop story wasn't Russian disinformation designed to illegitimately sway the election.[167] Although that fear turned out to be misplaced,[168] it shows the vital role that social media companies, and perhaps other intermediaries, play in *protecting* American democracy from undue influence by users, both foreign and domestic, through their content moderation practices.[169]

But more importantly, arguments for applying First Amendment principles to private platforms ignore what makes governments different: their plenary power. YouTube can ban certain conspiracy theories but only on its site, leaving society free to investigate whether they're true elsewhere. Facebook could amplify only pro-Democrat news articles if it wanted, but pro-Republican articles could still be published and discussed online. Only government can truly shackle the search for truth or frustrate

---

164. *See* Zeynep Tufecki, *It's the (Democracy-Poisoning) Golden Age of Free Speech*, WIRED (Jan. 16, 2018, 6:00 AM), https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/ [https://perma.cc/RY8T-KWZQ]; *see also* Bridy, *supra* note 8, at 217–18.

165. *See* Danielle K. Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 72–77 (2009) (describing real-world accounts in which harassing and threatening speech caused women to voluntarily shut down their websites).

166. Sean Illing, *"Flood the Zone with Shit": How Misinformation Overwhelmed Our Democracy*, VOX (Feb. 6, 2020, 9:27 AM), https://www.vox.com/policy-and-politics/2020/1/16/20991816/impeachment-trial-trump-bannon-misinformation [https://perma.cc/7CKF-2NLQ].

167. *See* Ken Dilanian, *Feds Examining Whether Alleged Hunter Biden Emails Are Linked to a Foreign Intel Operation*, NBC NEWS (Oct. 15, 2020, 5:42 PM), https://www.nbcnews.com/politics/national-security/feds-examining-if-alleged-hunter-biden-emails-are-linked-foreign-n1243620 [https://perma.cc/K498-QZDJ] (explaining why federal agents were concerned that information discovered on the laptop could have been part of a foreign intelligence operation).

168. *See* Kenneth Garger, *Hunter Biden's Infamous Laptop Confirmed in New York Times Report*, N.Y. POST (Mar. 17, 2022, 4:20 AM), https://nypost.com/2022/03/17/hunter-bidens-infamous-laptop-confirmed-in-new-york-times-report/ [https://perma.cc/495J-A9W6].

169. *See, e.g.*, *Reddit Apologises for Online Boston 'Witch Hunt'*, BBC (Apr. 23, 2013), https://www.bbc.com/news/technology-22263020 [https://perma.cc/3V2K-MZD7] (describing the harm that resulted when a Reddit community attempted to crowdsource the investigative work of identifying those responsible for the Boston Marathon bombing).

the enterprise of self-government because only government can use the coercive power of the law to stifle free speech in all venues. Thus, unless private parties are endowed with the power to dictate what can be said *throughout* the internet,[170] First Amendment principles, by themselves, don't provide a solid theoretical foundation for interventionism.

2. Non-Discrimination

Non-discrimination provides another potential basis for intervening on behalf of users.[171] After all, a provider's decision to allow certain statements or users but not others is undeniably a discriminatory act. The question is whether such discrimination should be regulated.

The answer to this question depends on whether non-discrimination laws that might be applied to internet activities should rest on a deontological foundation or an economic foundation. Deontologically-based non-discrimination regimes operate from the principle that discriminating against individuals or groups based on certain immutable or deeply personal characteristics is morally repugnant to the dignity of those who are excluded.[172] Thus, under the 1964 Civil Rights Act,[173] the Pregnancy Discrimination Act,[174] and the Americans with Disabilities Act of 1990[175]—all examples of deontologically-based non-discrimination regimes—public and private entities are prohibited from discriminating based on, *inter alia*, race, religion, national origin, pregnancy status, or disability.

To these protected characteristics, some interventionists would add another: ideology. A growing number of those on the political right, for example, allege that large, west coast technology providers routinely censor conservative viewpoints,[176] while some allege that it is rather left-

---

170. *See infra* section II.A.

171. For examples of scholars and commentators who have entertained using non-discrimination law (whether economic or deontological) to regulate online platforms (not including ISPs), see authorities cited *supra* note 5.

172. *E.g.*, BENJAMIN EIDELSON, DISCRIMINATION AND DISRESPECT 6–8 (2015); DEBORAH HELLMAN, WHEN IS DISCRIMINATION WRONG? 6–8 (2008).

173. Pub. L. No. 88-352, 78 Stat. 241 (1964).

174. Pub. L. No. 95-555, 92 Stat. 2076 (1978).

175. Pub. L. No. 101-336, 104 Stat. 327 (1990).

176. *E.g.*, Chuck Grassley, Senator, Floor Remarks: Big Tech, Media Continues to Censor Conservatives (Feb. 17, 2022), https://www.grassley.senate.gov/news/remarks/grassley-big-tech-media-continues-to-censor-conservatives [https://perma.cc/5SGU-RXFC]; KARA FREDERICK, HERITAGE FOUND., COMBATING BIG TECH'S TOTALITARIANISM: A ROAD MAP 2–3 (2022), https://www.heritage.org/sites/default/files/2022-02/BG3678.pdf [https://perma.cc/8P89-5SDU].

leaning viewpoints that are being suppressed.[177] Calls have therefore increased to require certain providers to welcome all viewpoints, and some aggrieved users have even sued social media companies for ideological discrimination under public accommodation laws.[178]

But those who would use existing public accommodation laws to regulate content moderation must clear two non-trivial hurdles. First, they must establish that online services constitute public accommodations. Title II of the 1964 Civil Rights Act, for example, pertains to inns, restaurants, theaters, and the like as well as establishments "physically located within" any of the foregoing.[179] While some courts have interpreted the Americans with Disabilities Act to require operators to make their websites accessible to users with disabilities,[180] no litigant has thus far persuaded any court to extend Title II to virtual spaces, such as websites.[181]

State laws provide more fertile ground for treating websites as public accommodations,[182] but even if that predicate is satisfied, litigants must clear the second hurdle: establishing ideology as a protected classification. Again, federal law takes a conservative approach while state laws experiment at the margins. Title II recognizes only race, color, religion, and national origin as protected classes.[183] While most states more or less mimic Title II in that regard, a handful of states, territories, counties, and cities also include political ideology as a protected characteristic. For example, the D.C. Human Rights Act prohibits discrimination based on "political affiliation,"[184] and certain Maryland counties protect "political

177. *See* Emily A. Vogels, Andrew Perrin & Monica Anderson, *Most Americans Think Social Media Sites Censor Political Viewpoints*, PEW RSCH. CTR. (Aug. 19, 2020), https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/ [https://perma.cc/33MQ-Q5X6] ("19% [of Democrats] say conservative sentiments are the ones that are more valued [by major technology companies].").

178. *See* Adi Robertson, *Social Media Bias Lawsuits Keep Failing in Court*, VERGE (May 27, 2020, 2:43 PM), https://www.theverge.com/2020/5/27/21272066/social-media-bias-laura-loomer-larry-klayman-twitter-google-facebook-loss [https://perma.cc/EM32-64ES].

179. Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241, tit. II, § 201(b) (1964) (codified as 42 U.S.C. § 2000a(b)).

180. *E.g.*, Robles v. Domino's Pizza, LLC, 913 F.3d 898, 904–06 (9th Cir. 2019); Nat'l Fed'n of the Blind v. Scribd Inc., 97 F. Supp. 3d 565, 575–76 (D. Vt. 2015); Nat'l Ass'n of the Deaf v. Netflix, Inc., 869 F. Supp. 2d 196, 201–02 (D. Mass. 2012).

181. *E.g.*, Martillo v. Twitter, Inc., No. 21-11119, 2021 WL 8999587, at *1 (D. Mass. Oct. 15, 2021); Lewis v. Google LLC., 851 Fed. Appx. 723, 724 (9th Cir. 2021).

182. *See* DAVID BRODY & SEAN BICKFORD, LAW.'S COMM. FOR CIV. RIGHTS, DISCRIMINATORY DENIAL OF SERVICE: APPLYING STATE PUBLIC ACCOMMODATIONS LAWS TO ONLINE COMMERCE 2 (2020), https://lawyerscommittee.org/wp-content/uploads/2019/12/Online-Public-Accommodations-Report.pdf [https://perma.cc/GPW5-R7M2].

183. 42 U.S.C. § 2000a(a).

184. D.C. CODE §§ 2-1401.02(25), 2-1402.31(a) (2023).

opinion," defined as "the opinions of persons relating to government, or the conduct of government; or related to political parties authorized to participate in elections in the State."[185] But given the vanishingly small overlap between public accommodation laws that pertain to online services and laws that protect general ideology—if indeed such an overlapping space even exists—it appears that no litigant has yet prevailed in a claim against an online provider for "ideological censorship."[186]

With few options available under traditional public accommodation laws, some states have tried to fill the gap, passing laws specifically protecting users from ideological discrimination by large technology providers, such as Facebook and Google. Florida's law, for instance, prohibits certain social media platforms from banning political candidates or "journalistic enterprises."[187] And Texas's H.B. 20 makes it illegal for social media companies with fifty million or more monthly users to ban users based on their viewpoints.[188] Similar federal bills have been proposed.[189] But even if such state laws survive the First Amendment—Florida's law has already been preliminarily enjoined[190]—they face other problems. Section 230 largely immunizes online service providers from liability for content moderation decisions taken in good faith, preempting contrary state laws.[191] And even if such laws could successfully skirt Section 230, they might not survive the dormant Commerce Clause.[192]

But far more interesting for our purposes is the theory underlying such laws. Assuming a deontological foundation, it's hard to argue that prohibiting, say, antisemitic epithets on a private internet platform represents a clear moral harm, or at least one that outweighs the moral harm to others on the platform who might have to endure the abuse. Legislators could try to avoid such a result by limiting protection to

185. PRINCE GEORGE'S CNTY., MD. CODE §§ 2-186(a)(23), 2-220 (2023).

186. *E.g.*, Freedom Watch, Inc. v. Google, Inc., 368 F. Supp. 3d 30 (D.D.C. 2019).

187. FLA. STAT. §§ 501.2041(h), (j) (2022).

188. TEX. CIV. PRAC. & REM. CODE ANN. §§ 143A.002, 143A.004(c) (West 2021).

189. *See, e.g.*, Jane Coaston, *A Republican Senator Wants the Government to Police Twitter for Political Bias*, VOX (June 26, 2019, 3:30 PM), https://www.vox.com/2019/6/26/18691528/section-230-josh-hawley-conservatism-twitter-facebook [https://perma.cc/94WW-4H9S] (describing a Republican-sponsored bill that would effectively prevent certain social media companies from moderating content "in a politically biased manner").

190. *See* NetChoice, LLC v. Att'y Gen. of Fla., 34 F.4th 1196, 1231 (11th Cir. 2022). *But see* NetChoice, LLC. v. Paxton, 49 F.4th 439, 459, 494 (5th Cir. 2022) (declining to enjoin Texas's law).

191. 47 U.S.C. § 230(e)(3).

192. *But see* Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation* (Harvard L. Sch. Pub. L. Working Paper, Paper No. 22-21, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4142647 [https://perma.cc/U9KK-JWBG] (arguing that certain state laws regulating online services might not run afoul of the dormant Commerce Clause).

political opinions, but doing so would only highlight a deeper definitional problem. Antisemitism, like white supremacy or even violent anarchy, is no less a political opinion merely because it lacks a formal political party or other traditional forms of organization. In fact, any imaginable viewpoint could conceivably qualify as a political opinion, a fact supported by the Supreme Court's nearly limitless conception of what constitutes political speech.[193]

One way to avoid the absolutism inherent in the deontologically-based non-discrimination regimes now favored by the right is to place non-discrimination theory on an economic foundation instead, an approach long favored by those on the left.

Under the law of common carriage, certain firms may be prevented from discriminating against lawful customers, depending on the nature of the firm or its industry. Historical bases for common carriage include when an industry is affected with the public interest, when a natural monopoly exists, or when a firm holds itself out as being open to the public—though scholars have criticized each such basis, and courts have not been consistent in their application.[194] Most importantly, for our purposes, the Federal Communications Act,[195] as amended, subjects telecommunications service providers to common carriage requirements, including non-discrimination mandates, rate regulation, and interconnection obligations.[196]

That internet service was not regulated as a telecommunications service—and, thus, not subject to common carriage—was not terribly controversial for much of the internet's history. Indeed, it was in keeping with the predominant view through the 1990s—shared by both the left and the right—that the internet should generally remain free from government interference.[197] That consensus began to fracture, however, after several ISPs were found to have leveraged their power over their own networks to disadvantage providers that offered competing value-added services. In 2005, for example, a North Carolina DSL provider prevented its customers from using Vonage's Voice-over-Internet-Protocol phone

193. *See generally* Morgan N. Weiland, *Expanding the Periphery and Threatening the Core: The Ascendant Libertarian Speech Tradition*, 69 STAN. L. REV. 1389 (2017).

194. *See* Yoo, *Common*, *supra* note 69, at 994–96.

195. 47 U.S.C. §§ 151–646 (1934) (amended 2021).

196. *See* 47 U.S.C. §§ 201–276.

197. *See* 47 U.S.C. § 230(b) ("It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation . . . ."); *see also* 141 CONG. REC. 16242 (1995) (showing broad bipartisan support for the 1996 Telecommunications Act, which included Section 230); Yoo, *Common*, *supra* note 69, at 992 (explaining that net neutrality proponents initially resisted subjecting internet access services to regulation via common carriage).

service.[198] In 2007, Comcast began blocking traffic between peer-to-peer filesharing applications.[199] And other ISPs, including mobile service providers, began striking deals through which third-party content providers could pay to exempt their web traffic from subscribers' data caps ("zero-rating")[200] or to prioritize their traffic over that of other content providers ("paid prioritization").[201]

In response, proponents of "net neutrality" began pushing for regulation that would force ISPs to treat all internet traffic alike.[202] And in 2015, the FCC's Open Internet Order reclassified broadband internet access as a telecommunications service subject to common carriage requirements.[203] The 2015 Open Internet Order included *ex ante* rules prohibiting broadband internet access service providers from blocking or throttling lawful content, applications, services, or non-harmful devices or favoring certain lawful internet traffic over other lawful traffic in exchange for consideration.[204] That regulatory achievement, however, was soon to be undone when the Trump-era FCC promulgated the 2017 Restoring Internet Freedom Order, which reversed the classification, freeing ISPs once again from common carriage requirements.[205]

Despite the volatility of federal net neutrality rules, some proponents of user-centric interventionism have suggested regulating certain online service providers as common carriers to protect users from discrimination.[206] Common carriage, it is believed, might provide a better theoretical basis for non-discrimination because only those providers that meet certain narrow criteria would fall into scope. Other providers would remain free to discriminate in furtherance of their editorial, ideological, or other interests.

For example, Richard Epstein has argued that "social-media giants,"

---

198. Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, ¶ 65 n.69 (2015) [hereinafter 2015 Open Internet Order].

199. Declan McCullagh, *FCC Formally Rules Comcast's Throttling of BitTorrent Was Illegal*, CNET (Aug. 20, 2008, 4:33 PM), https://www.cnet.com/tech/tech-industry/fcc-formally-rules-comcasts-throttling-of-bittorrent-was-illegal/ [https://perma.cc/XPX5-HLTS].

200. *See* 2015 Open Internet Order, *supra* note 198, ¶ 151.

201. *Id.* ¶¶ 19, 82, 127.

202. *See, e.g.*, Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 166–71 (2003) (coining the term "network neutrality" and proposing a model non-discrimination law).

203. 2015 Open Internet Order, *supra* note 198, ¶ 59.

204. *Id.* ¶¶ 14–18.

205. *See* Restoring Internet Freedom, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd. 311, ¶¶ 1–5 (2017).

206. *See* Volokh, *supra* note 2; Varadarajan, *supra* note 2; Rahman, *supra* note 5; McCabe, *supra* note 5.

such as Twitter and Facebook, and potentially mobile app store operators, such as Apple and Google, should be subject to common carriage requirements based on "the common-law rule . . . that 'no private monopoly has the right to turn away customers.'"[207] In Epstein's view, because these companies dominate their respective markets, such "near-monopoly position[s]" should have prevented Twitter from banishing Donald Trump, Apple from removing Gab from its app store, and Facebook from setting rules about what users can and cannot post.[208] Similarly, Frank Pasquale believes the "massive" size of certain internet companies, coupled with the fact that such companies hold themselves out as open to the public, justifies regulating them as "digital utilities."[209] Pasquale's "platform neutrality" regime would mimic or extend net neutrality, which concerns only the internet access market, to dominant social media platforms, search engines, and even online marketplaces.[210]

But net neutrality is a poor model for remedying ideological discrimination by website operators. From its earliest days, net neutrality has always concerned itself with competitive rather than moral harms and with network management rather than content moderation. The ideal regulatory target of net neutrality is the ISP that offers an "over-the-top" (and often higher-margin) application, such as digital telephony or streaming video, in addition to its primary (and often lower-margin) internet access service. Net neutrality would prevent that ISP from leveraging its network to unfairly advantage its application, whether by zero-rating network traffic for the application, charging competitors for access to its customers, or blocking competitive applications altogether.

These competitive concerns are altogether absent when social media platforms, search engines, and mobile app store operators ground their content moderation decisions on ideological commitments. When Twitter and Facebook suspended Donald Trump from their platforms, they did so because they believed his "stop the steal" rhetoric risked fomenting imminent violence,[211] not because he offered a competitive social media platform that threatened to steal users and advertisers. When YouTube

---

207. Varadarajan, *supra* note 2 (quoting Richard Epstein).

208. *Id.*

209. Frank Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, 17 THEORETICAL INQUIRIES L. 487, 490 (2016).

210. *Id.* at 497–503; *see also* Daisuke Wakabayashi & Cecilia Kang, *Ohio's Attorney General Wants Google to Be Declared a Public Utility*, N.Y. TIMES (June 8, 2021), https://www.nytimes.com/2021/06/08/technology/google-ohio-public-utility.html (last visited Apr. 10, 2023).

211. *Permanent Suspension of @realDonaldTrump*, TWITTER (Jan. 8, 2021), https://blog.twitter.com/en_us/topics/company/2020/suspension [https://perma.cc/TKQ2-J3KW] ("[W]e have permanently suspended the account due to the risk of further incitement of violence.").

removed more than half a million videos that allegedly contradicted expert consensus on COVID-19, it did so to protect public health from medical misinformation,[212] not because those content providers refused to pay digital tolls to access Google's users.

Instead, as Christopher Yoo has shown, common carriage works best under a narrow set of circumstances. Those circumstances include when:

1. The product being regulated is a commodity;
2. The interfaces between the product being regulated and related products are simple;
3. The transmission technology is uniform and stable;
4. The transmission network is fully built out; and
5. The demand for each firm producing the regulated product is relatively stable.[213]

The absence of these factors for most internet applications—social media services, for example, are hardly commodities—shows that common carriage is a poor fit for most online service providers. More broadly, it illustrates the awkwardness that results from attempting to repurpose economic tools to address what is ultimately a moral concern when providers discriminate based on ideology. It also shows that economics is a poor foundation on which to build a non-discrimination theory of interventionism, at least when it comes to the application layer of the internet.[214]

3. User Property Rights

Finally, intervention could be premised on users' own property rights. In 2000, John Perry Barlow declared, "[t]he future will win; there will be no property in cyberspace."[215] While Barlow's prediction spoke to intellectual property—he longed for a future "DotCommunism" that would prevent content owners from enforcing their copyrights online[216]—his words already rang true when it came to cyber-property. From the beginning, one of the most remarkable—yet least considered—aspects of cyberspace has been its unpropertied nature. Some scholars have

---

212. Richard Nieva, *YouTube Says It's Removed 500,000 COVID-19 Misinformation Videos*, CNET (Jan. 26, 2021, 6:00 AM), https://www.cnet.com/tech/tech-industry/youtube-says-its-removed-500000-covid-19-misinformation-videos/ [https://perma.cc/E6AC-SSG6].

213. Yoo, *Common*, *supra* note 69, at 994.

214. *See* section II.A.1 (describing the application layer).

215. John Perry Barlow, *The Next Economy of Ideas*, WIRED (Oct. 1, 2000, 12:00 PM), https://www.wired.com/2000/10/download/ [https://perma.cc/6KHD-C9PA].

216. *Id.*

bemoaned the lack of public property on the internet.[217] Unlike real space, cyberspace offers no public parks for rallies or sidewalks on which users can picket next to private online establishments.[218] But far more concerning, I would argue, is the fact that no *private* property exists on the internet.

To be sure, users and providers can own physical property, which they can use to communicate over the internet—servers, client devices, and network cables, for instance—although as discussed above, the digital divide places far more of that physical property in the hands of providers.[219] And intellectual property can attach to online activities—copyrights in streaming content, trademarks in domain names, and patentable processes in network applications—just as surely as it can attach to offline activities.

But when it comes to phenomena that can exist only online, such as webpages, user profiles, or digital storefronts, the absence of title-held property has profound implications. Consider the user who labors for years to build a successful online store, only for eBay to terminate her account without warning or explanation. Few would deny that her account termination represents a significant financial loss. We can envision similar losses, whether economic, reputational, or personal, in other scenarios: the Instagram celebrity who loses a million followers when his account is taken down; the activist website that sees its traffic drop by ninety percent after Google removes the site from its search results; users who are suddenly deprived of human connection and support when Facebook shutters a shared interest group page.[220] Yet each such provider could no doubt point to provisions in its terms of service stating that users acquire no property interests in anything they create within the service, whether handles or user followings (with some exceptions perhaps for their own content).[221] Every aspect of the service is just that—a *service*—and one

217. *See, e.g.*, Nunziato, *supra* note 81, at 1117–18 (arguing that the overwhelmingly private nature of cyberspace frustrates the traditional governmental enterprise of providing speakers with meaningful public forums).

218. *See* Noah D. Zatz, *Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment*, 12 HARV. J.L. & TECH. 149, 188 (1998) ("There is no room in these models for leafleting passers-by as they travel the Information Superhighway nor for picketing in front of cyber-stores.").

219. *See supra* section I.B.2.

220. *See, e.g.*, Kashmir Hill, *Many Are Abandoning Facebook. These People Have the Opposite Problem.*, N.Y. TIMES (Aug. 22, 2019), https://www.nytimes.com/2019/08/22/business/reactivate-facebook-account.html (last visited Apr. 11, 2023) (describing a terminated user who lost access to photos of his deceased brother).

221. *See, e.g.*, TWITTER, *Terms of Service*, *supra* note 21 ("All right, title, and interest in and to the Services (excluding Content provided by users) are and will remain the exclusive property of Twitter

that can be revoked at any time.

But the consequences of an unpropertied internet go deeper. In real space, static, title-held property can act as a failsafe for those marginalized by society. The heretic can pen his heterodoxy in books (personal property), which he can print and distribute by hand, and which can be passed down and read for generations without depending on commercial storage vendors or distributors. As a last resort, cultural outcasts can buy land (real property) and establish a self-supporting community without relying on intermediaries to speak to one another within their commune.[222] But because online resources and activities always require intermediaries to render continuous, real-time services, internet users can never be self-sufficient in the same way.[223]

While the law cannot remove these dependencies—the service-oriented nature of electronic communications not only defines the internet but is what makes the internet such a powerful medium—the law can restructure the power dynamics that result from them. By granting users certain property rights in their online resources, the law can protect users' interests, including their expressive interests, from the arbitrary power of online service providers.[224] Just as the CFAA strengthened the power of providers by codifying our intuition that hardware should be protected just as much from electronic interference as from physical trespass, the law could correspondingly strengthen the rights of users by codifying similar intuitions about what feel like user property interests.

For example, registrars have increasingly taken to seizing domain names when registrants use them in connection with offensive, albeit lawful, websites.[225] As a result, in a previous work, I argued for treating domain names as personal, title-held property to protect website operators from "DNS censorship" at the hands of providers.[226] Similar arguments

---

and its licensors."); CANADIAN INTERNET REGISTRATION AUTH., REGISTRANT AGREEMENT, VERSION NO. 2.2, § 3.2 (2022), https://static.cira.ca/policy/Registrant%20Agreement%20Version%202.2_0.pdf [https://perma.cc/AWG8-UAKG] ("The Registrant acknowledges and agrees that a Domain Name is not property and that a Domain Name Registration does not create any proprietary right for the Registrant.").

222. *See infra* section II.B.

223. *See* Derek Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 910 (2012) ("Speech requires space. American constitutional jurisprudence recognizes that speakers need a place where they can reach an audience.").

224. *Cf.* Lessig, *supra* note 6, at 520 ("The state could (1) give individuals a property right to data about themselves, and thus (2) create an incentive for architectures that facilitate consent before turning that data over.").

225. *See infra* section III.B.3; *see also* Nugent, *supra* note 114, at 73–75. As further explained in section III.B.3, a domain registrar is an entity that provides domain name registration services.

226. *See generally* Nugent, *supra* note 114.

could be made for Internet Protocol (IP) addresses.[227]

But while a theory of interventionism premised on user property rights works well for domain names and IP addresses, it might be difficult to extend such a theory to other types of online resources. No secondary market exists for YouTube accounts, nor can a LinkedIn influencer sell her subscriber base to another user. While domain names can exist separate and apart from individual registrars, users cannot migrate their Twitter handles to other platforms. These types of online resources are application-specific and provider-dependent. The law could not grant users property rights in such resources without forcing those providers to perpetually provide services against their will. Accordingly, although property rights should play some role in ensuring that unpopular users can continue to express themselves online, they cannot serve as the foundation for a comprehensive interventionist framework.

* * *

To summarize, each of the interventionist theories reviewed above has obvious merits, but each such theory is sufficiently flawed that it fails to adequately explain when and how the law should intervene in private content moderation. And, importantly, none of these theories seems to balance both user and provider rights effectively.

As such, it might be tempting to simply default to a "Free Market Plus" baseline—that is, a generally deregulatory environment plus minor tweaks, such as Section 230's protection against debilitating secondary liability.[228] In other words, perhaps the system we have today is the *least bad option* for addressing content moderation. This system effectively provides no legal rights for users, but that might be insoluble. The risk of flooding websites with the worst kinds of extremist content might simply be too high if the state begins tinkering with the machinery of content moderation. And as for free speech, we can take hope in the fact that there will always be some place on the internet for any speaker, no matter how extreme or heterodox, to express their viewpoints.

But before we abandon the search for a unifying theory of interventionism that can balance both user and provider rights, it's worth questioning this last assumption. If users don't have any content rights against private providers on the internet, then should there be *no* limits to how far those providers can go in targeting unpopular user speech? And are we certain that unpopular users will *always* be able to find some forum on the internet in which to express their views?

227. *See id.* at 105–06.

228. *See* Lemley, *supra* note 40, at 325–26.

In the next Part, I test this assumption and explore these questions by examining the phenomenon of viewpoint foreclosure, the systematic removal of certain lawfully expressed viewpoints from the internet. By focusing on this emerging problem, I argue that we can, at the very least, build an account of certain core or minimum user content rights against private providers.

II. VIEWPOINT FORECLOSURE AND THE INTERNET STACK

If content moderation today looked like content moderation ten or fifteen years ago, then a Free Market Plus framework might indeed be the right approach to regulation. If one provider moderates too aggressively, then other providers can make a play for dissatisfied users by offering more lax content policies. A deregulated environment that allows a diverse array of acceptable use policies to flourish will more likely accommodate differing user and provider interests than a one-size-fits-all approach that might come from regulation. And even if most of the industry coalesces organically on a common set of content policies, some fraction of niche providers will still cater to heterodox users who remain shut out of mainstream websites. Or, as a last resort, a truly beleaguered user can always stand up her own website on which she can express her views.

But content moderation has not remained static. On the contrary, it has evolved and expanded in ways that challenge these central free market assumptions. Whereas users could previously expect that their right to use a popular website depended solely on how they behaved on that website, deplatforming now scrutinizes users' general reputations, offsite behavior, and personal associations. Whereas content moderation once limited itself to individual websites, modern no-platforming campaigns chase unpopular speakers from site to site. Whereas providers have traditionally decided for themselves which content to allow or deny, deep deplatforming now seeks to impose uniform standards by pressuring infrastructure vendors to terminate essential services to websites that refuse to deplatform unpopular speakers. And whereas users could always escape deep deplatforming by vertically integrating and creating their own websites, viewpoint foreclosure now threatens to make even that remaining option unavailable by depriving certain speakers of the core infrastructural resources on which all websites depend.

This dramatic expansion in the scope of content moderation raises an important question that internet scholars must confront. Even if this extreme level of deplatforming is generally reserved for the most offensive online speech—what some have called "lawful but awful"

content[229]—should Good Samaritanism have *no* limiting principle? When, if ever, does well-intentioned content moderation go too far, such that the law should step in to stop it?

I argue that content moderation crosses an important line once it reaches the level of viewpoint foreclosure—when private intermediaries effectively prevent a person or group from publishing a particular viewpoint on the internet altogether. But before making that case, it is first necessary to show *how* viewpoint foreclosure may occur. Therefore, in this Part, I explain the mechanics of viewpoint foreclosure using two analytical tools. First, I employ a running case study of a fictional user who wishes to express certain unpopular viewpoints on the internet but is prevented from doing so. Second, I suggest a three-layer "internet stack" as a useful heuristic for understanding the architecture of content moderation.

In one sense, viewpoint foreclosure represents just the next step in the evolution of content moderation, albeit the most extreme and exclusionary form of it. Thus, I have constructed the case study to illustrate that evolution as it progresses through four distinct stages: classic content moderation, deplatforming, deep deplatforming, and finally viewpoint foreclosure, with each stage capturing more real estate within the internet stack.

A. The Evolution of Content Moderation

1. Classic Content Moderation

Our story begins with Jane, a typical internet user in the United States who, one day, chances upon a centuries-old manifesto in a local bookstore that fundamentally alters her worldview. After first discussing it with friends and family over email, WhatsApp, and Zoom, as well as in person, the contours of her new political philosophy take shape, and she decides to use the internet to evangelize it more broadly.

Jane starts with Facebook, her mainstay for discussing politics online. In time, she develops a following; a small but growing crop of other users begins to engage with her content. Unfortunately for Jane, however, her new worldview is decidedly outside the mainstream. Perhaps, convinced that the current political process is hopelessly stacked against marginalized groups, she advocates for obstructing the police or calls for the violent overthrow of capitalism, albeit in ways that fall short of incitement. Perhaps she cheers on terrorism or opposes it to the point of

229. Eric Goldman & Jess Miers, *Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules*, 1 J. FREE SPEECH L. 191, 194 n.12 (2021).

embracing racial or religious profiling. Perhaps she espouses outlandish conspiracy theories or spouts information about vaccines or diseases that is widely regarded as incorrect. But whatever her precise ideology—whether far-left or far-right, whether expressed thoughtfully or vituperatively—her viewpoint is sufficiently heterodox that most people find it offensive and even dangerous, including Facebook. And in due course, after many complaints from users who encounter her posts, Facebook steps in to limit the spread of Jane's content.

Here we see classic content moderation in action, as defined by two variables: the scope of concern and the scope of action. At this point, Facebook has concerned itself only with Jane's conduct on its site and whether that conduct violates Facebook's acceptable use policies (scope of concern). Next, having decided that Jane has violated those policies, Facebook solves the problem by simply deleting Jane's content from its servers, preventing other users from accessing it, and/or terminating Jane's account (scope of action). But importantly, these actions take place solely within Facebook's site, and once booted, Jane remains free to join any other website. Thus, as depicted in Figure 2, classic content moderation is characterized by a narrow scope of concern and a narrow scope of action, both of which are limited to a single site.

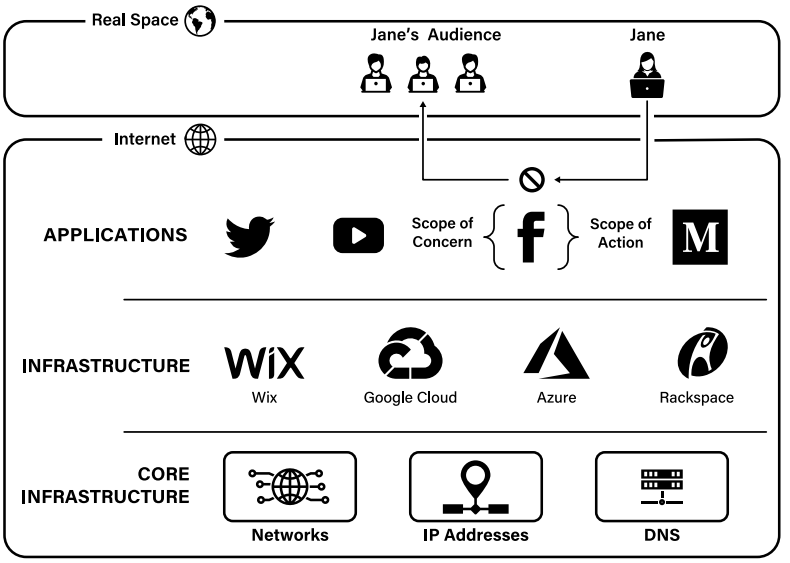

Figure 2 – Classic Content Moderation

Figure 2 also introduces the concept of the three-layer internet stack,

which we'll reference throughout this case study.[230] The "internet stack," as I've defined it, comprises an application layer, an infrastructure layer, and a core infrastructure layer. The application layer contains the universe of applications that make content directly available to consumers, including messaging apps, games, and, most importantly for our purposes, websites. Just below, sits the infrastructure layer, which provides the resources on which all internet applications depend, including hosting, storage, hardware, and software. Finally, at the bottom of the stack, the core infrastructure layer contains the core internet resources on which the infrastructure layer depends, including networks, IP addresses, and DNS (domain names).

2. Deplatforming

Because classic content moderation is confined to the boundaries of Facebook's own site, Jane remains free to migrate to another online forum to express her viewpoint. She does this by creating accounts on other social media networks, such as Twitter and YouTube, and by building a presence on Medium, a more traditional blogging platform. Also, chastened by her expulsion from Facebook, she decides to play it coy for a while. She accumulates followers on these other platforms using less controversial content while reserving her most incendiary remarks for offline activities, including rallies, television appearances, and even a self-published book. However, despite flying just below the line that separates permitted from prohibited content, Jane soon finds herself expelled from these additional platforms. Why?

Here we see the primary distinction between classic content moderation and modern deplatforming. Whereas the former remains fairly confined to the website at issue, deplatforming may entail onsite consequences for offsite speech or conduct. As one dictionary aptly put it, to deplatform is "to prevent a person who holds views that are not acceptable to many people from contributing to a debate or online forum."[231] Deplatforming, thus, targets users or groups based on the ideology or viewpoint they hold, even if that viewpoint is not expressed on the platform at issue. For example, in April 2021, Twitch updated its terms of service to reserve the right to ban users "even [for] actions [that] occur entirely off Twitch,"

---

230. This heuristic, offered only for illustration, is distinct from other conceptual models of the internet, such as the five-layer "TCP/IP" stack or the seven-layer "OSI" stack.

231. *Deplatform*, OXFORD LEARNER'S DICTIONARIES, https://www.oxfordlearnersdictionaries.com/us/definition/english/deplatform [https://perma.cc/52LF-W58Y].

such as "membership in a known hate group."[232] Under these terms, mere membership in an ideological group, without any accompanying speech or conduct, could disqualify a person from the service. Other prominent platforms have followed suit in their terms of service, and enforcement actions have included demonetizing a YouTube channel after its creators encouraged others (outside of the platform) to disregard social distancing,[233] suspending Facebook and Instagram accounts for those accused (but not yet convicted) of offsite crimes,[234] terminating the Patreon account of a user who uttered a racial slur on another platform,[235] and banning a political pundit (and her husband) from Airbnb after she spoke at a controversial (offline) conference.[236]

Thus, although Jane had not yet violated any rules on Twitter or Medium, Jane's reputation may simply have preceded her. After learning that she had been kicked off Facebook and moved her operation elsewhere, Jane's detractors may have notified these platforms of Jane's past statements and behavior, both online and offline. And, not wishing to host a user known to have extreme views, these platforms elected to deny her a forum, even for her innocuous content. Using our model of the three-layer internet stack, and as depicted in Figure 3, we might say that deplatforming expands the scope of concern both horizontally, by examining users' conduct on other applications, and vertically, by penalizing users even for offline conduct.

---

232. *Our Plan for Addressing Severe Off-Service Misconduct*, TWITCH (Apr. 7, 2021), https://blog.twitch.tv/en/2021/04/07/our-plan-for-addressing-severe-off-service-misconduct/ [https://perma.cc/GZ6P-QSTM].

233. *See* @TeamYouTube, TWITTER (Sept. 11, 2020, 5:17 PM), https://twitter.com/TeamYouTube/status/1304574812833091584 (last visited Apr. 12, 2023).

234. *See* Vanessa Romo, *Meta Is Reversing Policy that Kept Kyle Rittenhouse from Facebook and Instagram*, NPR (Dec. 14, 2021, 8:46 PM), https://www.npr.org/2021/12/01/1060635724/meta-facebook-instagram-kyle-rittenhouse [https://perma.cc/F6WM-TLME].

235. *See* Benjamin Goggin, *Crowdfunding Platform Patreon Defends Itself from Protests by 'Intellectual Dark Web,' Publishes Slur-Filled Posts from Banned YouTuber*, BUS. INSIDER (Dec. 18, 2018, 4:11 AM), https://www.businessinsider.com/patreon-crowdfunding-platform-defends-itself-amid-boycott-2018-12 [https://perma.cc/4RTC-47YW].

236. *See* Zachary Petrizzo, *Michelle Malkin Banned from Airbnb After Attending Hate Fest*, DAILY BEAST (Feb. 3, 2022, 1:21 AM), https://www.thedailybeast.com/michelle-malkin-banned-from-airbnb-after-attending-hate-fest [https://perma.cc/PUR9-JJXC]; *see also* Chelsea Bailey, *Laura Loomer Banned from Uber & Lyft After Anti-Muslim Tweetstorm*, NBC NEWS (Nov. 2, 2017, 11:56 AM), https://www.nbcnews.com/news/us-news/laura-loomer-banned-uber-lyft-after-anti-muslim-tweetstorm-n816911 [https://perma.cc/WHB4-LXL4].

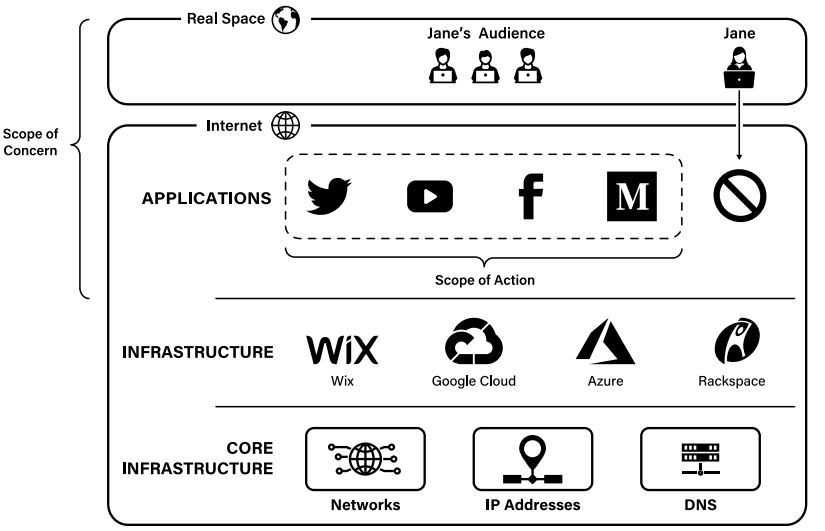

Figure 3 – Deplatforming / No-Platforming

While the scope of action remains the same in both classic content moderation and deplatforming—a website operator can still remove a problematic user only from its own site—we do see the scope of action expand horizontally if deplatforming progresses to no-platforming. As I use the term in this Article, no-platforming occurs when one or more third-party objectors—other users, journalists, civil society groups, for instance—work to marginalize an unpopular speaker by applying public pressure on any application provider willing to host the speaker. For example, Jane's detractors might mount a Twitter storm or threaten mass boycotts against any website that welcomes Jane as a user, chasing Jane from site to site to prevent her from having *any* platform from which to evangelize her views. As depicted in Figure 3, the practical effect of a successful no-platforming campaign is to deny an unpopular speaker access to the application layer altogether.

3. Deep Deplatforming

Having been shut out of every major platform, Jane now has two options. She can either migrate to a smaller, less influential third-party website or she can create her own. Both efforts, however, can effectively be stymied by deep deplatforming.

Jane decides to try her luck with a smaller outfit—nichehub.xyz—a

website that caters to misfits like herself and takes a more libertarian approach to content moderation. At first, this seems like an effective strategy. Although her detractors try to pressure NicheHub to drop Jane, just as they managed to pressure other website operators, NicheHub refuses, and Jane has once again gained entry to the application layer, the layer in which speech is made directly available to other users on the internet.

But NicheHub does not fully control its own fate. As a minor player in the online space, it lacks its own data centers and servers, relying instead on commercial hosting services provided by companies like Microsoft Azure, Google Cloud, Rackspace, and WiX. These providers offer infrastructure, such as computing and storage, on which customers can build and operate their own websites. Within hours of refusing to deplatform Jane, security researchers discover that NicheHub depends on these infrastructural providers and begin pressuring *them* to drop NicheHub as a customer. The campaign succeeds, and these providers give NicheHub twenty-four hours to cut ties with Jane before they turn the lights out on NicheHub's entire operation, a demand to which NicheHub reluctantly accedes.

Convinced she will suffer a similar fate if she migrates to any other third-party website, Jane decides to take matters into her own hands by registering the domain name radicaljane.chat and launching her own website. But eventually, this too proves futile. Like NicheHub, Jane's website requires infrastructural resources, such as hosting and storage. And just as infrastructural providers will not indirectly support her speech by selling hosting services to any website that offers her a platform, they will not directly support that same speech by welcoming her as a customer.[237]

These developments characterize deep deplatforming, a more aggressive form of deplatforming that uses second-order cancelation to plug the holes left by conventional techniques.[238] As depicted in Figure 4, deep deplatforming vertically expands both the scope of concern and the scope of action down to encompass the infrastructure layer of the internet stack. The practical effect is to prevent unpopular speakers from using *any* websites as platforms—even willing third-party websites or such speakers' own websites—by targeting those websites' technical dependencies.

---

237. *See, e.g.*, *Global Acceptable Use Policy*, RACKSPACE TECH. (Oct. 1, 2021), https://www.rackspace.com/information/legal/global/aup (last visited Apr. 27, 2023) (prohibiting customers from using Rackspace services to host websites that Rackspace regards as "morally repugnant").

238. *See* Zittrain, *supra* note 163.

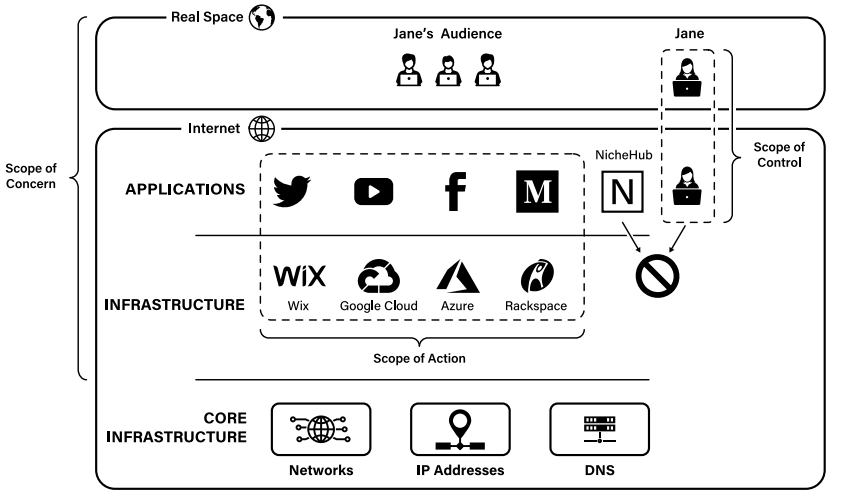

Figure 4 – Deep Deplatforming

Perhaps the most well-known instance of deep deplatforming concerned Parler, the alternative social network that styled itself as a free speech-friendly alternative to Facebook and Twitter. Following the January 6th Capitol riot, attention turned to Parler's alleged role in hosting users who amplified Donald Trump's "[s]top the [s]teal" rhetoric,[239] and pressure mounted against vendors that Parler relied on to stay online.[240] As a result, Amazon Web Services (AWS), a cloud computing provider on which Parler depended for hosting and other infrastructural services, gave Parler twenty-four hours to find another cloud provider.[241] When Parler proved unable to find a substitute before that deadline, AWS terminated services, taking Parler, along with all its users, offline.[242]

---

239. *See* Candace Rondeaux & Ben Dalton, *What Role Did the Far-Right Platform Parler Play in the Jan. 6 Insurrection?*, SLATE (Jan. 6, 2022, 10:14 AM), https://slate.com/technology/2022/01/parler-jan-6-capitol-facebook-twitter.html [https://perma.cc/2EPF-7CGV].

240. *See* Rudy Takala, *Apple Gives Parler 24 Hours to 'Improve Moderation'—or Get Kicked Off App Store*, MEDIAITE (Jan. 8, 2021, 6:58 PM), https://www.mediaite.com/news/just-in-apple-gives-parler-24-hours-to-improve-moderation-or-get-kicked-off-app-store/ [https://perma.cc/8KHW-UBVL].

241. *See* Darrell Etherington, *Parler Is Officially Offline After AWS Suspension*, TECH CRUNCH (Jan. 11, 2021, 7:51 AM), https://techcrunch.com/2021/01/11/parler-is-officially-offline-after-aws-suspension/ [https://perma.cc/D465-VURQ].

242. *Id.*; *see also* Thuy Ong, *Neo-Nazi Site Daily Stormer Threatened by Hosting Providers and Possible Hackers*, VERGE (Aug. 14, 2017, 4:39 AM), https://www.theverge.com/2017/8/14/16142384/daily-stormer-site-go-daddy-hosting-providers-hackers-anonymous [https://perma.cc/EYR4-ZSY3].

Figure 4 also introduces a new concept when it comes to evading deplatforming: the scope of control. As long as Jane depends on third-party website operators to provide her with a forum, she controls little. She can participate in the application layer—and thereby speak online—only at the pleasure of others. However, by creating her own website, she can extend her scope of control into the application layer, protecting her from the actions of other website operators (though not from the actions of infrastructural providers).

4. Viewpoint Foreclosure

At this point, Jane has one last shot to stay online: she can attempt to provide for her own infrastructure.[243] Leveraging donations she collected from users before her website was shut down, she purchases several professional-grade servers, rents rack space in a nearby colocation facility,[244] obtains commercial internet service from Lumen Technologies, and relaunches her website on an unsuspecting world.

Yet Jane never gets to see if her views can catch on. Her funding dries up when PayPal, Stripe, and other financial intermediaries refuse to process donations to her website. Lumen is identified by name in several online publications about Jane, and a Twitter campaign against Lumen ensues. Exercising its contractual right to distance itself from content that it decides is "inappropriate,"[245] Lumen gives Jane thirty days to find another ISP. In the meantime, Jane begins exploring whether she can bypass Lumen entirely by peering directly with a backbone network operator.[246] But she faces other obstacles.

After purchasing IP addresses and an autonomous system number on the secondary market, both of which she will need to create her own publicly accessible network, the regional internet registry associated with her network numbers revokes them. Her domain name, radicaljane.chat, is also taken from her when GoDaddy asserts its power to terminate service for domain names that generate an "excessive amount of

243. *Cf.* Jeremy W. Peters, *Rumble, the Right's Go-To Video Site, Has Much Bigger Ambitions*, N.Y. TIMES (Mar. 29, 2022), https://www.nytimes.com/2022/03/28/business/media/rumble-social-media-conservatives-videos.html (last visited Apr. 12, 2023) (noting that Rumble, an alternative social media network with more libertarian content moderation policies, "has already built out its own cloud service infrastructure and video streaming capacity, offering it and its partners greater independence from the Amazons and Microsofts of the internet").

244. A colocation facility is a data center in which multiple parties can rent space, power, and network connectivity for their servers and other equipment in lieu of building and operating their own data centers.

245. *See Lumen's Acceptable Use Policy*, LUMEN (Mar. 23, 2023), https://www.lumen.com/en-us/about/legal/acceptable-use-policy.html [https://perma.cc/9ZYN-3P3Z].

246. *See infra* section III.B.4 (explaining the role of a backbone network operator).

complaints" from the public or "result in damage to GoDaddy's . . . reputation."[247] Jane registers a new domain name—radicaljane.net—using a different provider, but she begins hearing that some of her users can no longer reach her website. Upon further investigation, she discovers that certain residential and mobile ISPs, such as Comcast and T-Mobile, are blocking users from accessing her website. She also learns that other users, whose ISPs are not blocking them, are nonetheless shut out because certain intervening backbone networks refuse to route packets to Jane's network.[248]

At this point, Jane has run out of options. She cannot replace these core infrastructural resources herself. She considers suing Lumen, GoDaddy, and the other providers who control these resources, but she is out of money. And even if she were not, she can find no law that these intermediaries violated.

It is this last set of actions that define viewpoint foreclosure, the final removal of Jane's website from the internet. As depicted in Figure 5, viewpoint foreclosure takes content moderation to its logical extreme by expanding the scope of action down to the core infrastructure layer. Although Jane expanded her scope of *control* into the infrastructure layer by obtaining her own hardware and software, she cannot go any deeper by constructing her own infrastructural resources. Her views have been effectively foreclosed on the internet.

247. *See Universal Terms of Service Agreement: Additional Reservation of Rights*, GODADDY (Mar. 20, 2023), https://www.godaddy.com/legal/agreements/universal-terms-of-service-agreement [https://perma.cc/48DV-ZWNC].

248. *See infra* section III.B.4 (explaining internet routing and the discretion networks have in their routing practices).

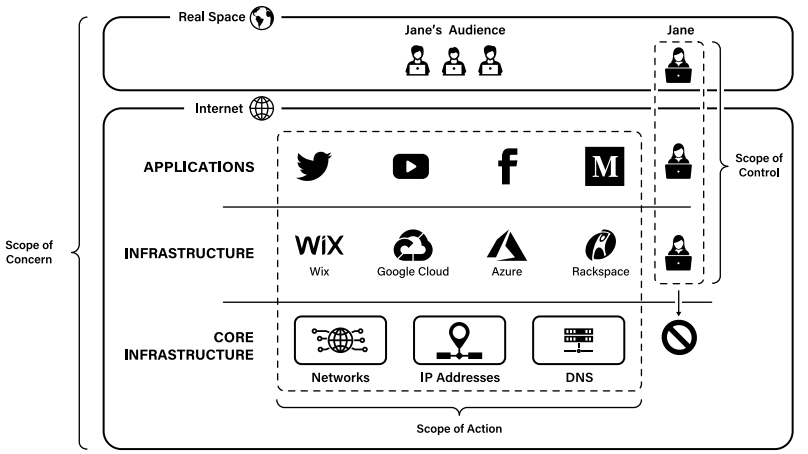

Figure 5 – Viewpoint Foreclosure

B. Examining Viewpoint Foreclosure

Viewpoint foreclosure challenges long-held assumptions about the give-and-take of content moderation. Central to the notion of keeping the government out of private content moderation is the assumption that a deplatformed speaker is never without recourse. If she gets kicked off a social media platform or other website because of her views, she can look for another third-party forum that will let her speak freely. If she cannot find an alternate provider, she can simply build her own website. She can even build features into her website that enable others to create and share content consistent with her viewpoint and, in so doing, build her own community. This failsafe—that any user can participate in online discourse by, as a last resort, hanging out her own shingle—has been a central premise since the early days of the internet.[249]

Deep deplatforming, by depriving unpopular speakers of certain building blocks, can make it harder to create competing platforms or websites, certainly, but the solution would seem to be the same: *vertical integration*. As vendors and resources become unavailable within each successive layer of the internet stack, a user determined to stay online can cobble together her own resources to compensate. Thus, a controversial organization could assemble its own servers, write its own protocol software, purchase its own IP addresses, and even stand up its own DNS

249. *Cf.* Reno v. ACLU, 521 U.S. 844, 870 (1997) (celebrating the web's potential to enable any user to become a "pamphleteer" or "town crier with a voice that resonates farther than it could from any soapbox").

nameservers. In other words, it could reach the vaunted status of being a full-stack rebel, that mythical online creature capable of withstanding all attempts to deplatform it.

Full-stack rebels have a long history in the offline world. Shunned by society or the established merchant class, a persecuted religious or racial group could, as a last resort, settle on separate land on which its adherents could live in a self-supporting community.[250] Radical political organizations whose manifestos were spurned by publishers could construct their own printing presses to churn out literature, which they could then distribute using their own vehicles (or feet).[251] Even if local paper and ink suppliers caught wind of such back-alley printing operations and refused to sell materials to them, a full-stack rebel could theoretically procure wood pulp to make her own paper and mix her own ink using countless ancient compounds.[252] Thus, short of violence or imprisonment, marginalized groups could often roll up their sleeves to provide for their own needs and thereby eke out an existence in real space, however humble.

But cyberspace is not like real space. Whereas offline rebels can vertically integrate down the real-space stack as deeply as necessary, online rebels who dig down the internet stack eventually hit bedrock—layers that inexorably depend on other parties. Whereas each stage of the

---

250. *See, e.g.*, HANNIBAL B. JOHNSON, BLACK WALL STREET: FROM RIOT TO RENAISSANCE IN TULSA'S HISTORIC GREENWOOD DISTRICT (2021) (describing various self-supporting African American settlements in between 1865 and 1920); MARK S. FERRARA, AMERICAN COMMUNITY: RADICAL EXPERIMENTS IN INTENTIONAL LIVING (2019) (chronicling the self-sufficient Zoarite community in rural Ohio); Shelly Tenenbaum, *Immigrants and Capital: Jewish Loan Societies in the United States, 1880–1945*, 76 AM. JEWISH HIST. 67, 68 (1986) (describing the "Hebrew free loan societies" that enabled Jewish residents to obtain otherwise unavailable capital to start businesses). Of course, I would be remiss not to acknowledge that the Tulsa Race Massacre of 1921 shattered much of the peace and security that had earlier been realized through the Black Wall Street collective. *See* Yuliya Parshina-Kottas, Anjali Singhvi, Audra D.S. Burch, Troy Griggs, Mika Gröndahl, Lingdong Huang, Tim Wallace, Jeremy White & Josh Williams, *What the Tulsa Race Massacre Destroyed*, N.Y. TIMES (May 24, 2021), https://www.nytimes.com/interactive/2021/05/24/us/tulsa-race-massacre.html (last visited Apr. 12, 2023).

251. *See, e.g.*, David R. Como, *Secret Printing, the Crisis of 1640, and the Origins of Civil War Radicalism*, 196 PAST & PRESENT 37, 38 (2007) (explaining the role of "clandestine presses that operated between 1644 and 1646" in fomenting Civil War radicalism); *A Brief Introduction to England's Secret Printing Presses*, HIST. ENG. BLOG (May 12, 2015), https://heritagecalling.com/2015/05/12/a-brief-introduction-to-englands-secret-printing-presses/ [https://perma.cc/L4HG-E9X2] (chronicling the role of secret printing presses in evading the censorship of heterodox ideas in England between 1450 and 1913).

252. *See* ALEXANDER MONRO, THE PAPER TRAIL: AN UNEXPECTED HISTORY OF A REVOLUTIONARY INVENTION (2016) (detailing historical innovations in papermaking and their role in producing social and political changes); JASON LOGAN, MAKE INK: A FORAGER'S GUIDE TO NATURAL INKMAKING (2018) (providing a history of inkmaking and explaining the science of distilling pigment from foraged materials, including soot, rust, and peach pits).

book printing and distribution process might be accomplished in a hundred different ways and use any one of thousands of different providers, certain internet functions can be performed in only one way or necessarily depend on only a few available providers. These limitations operate as "choke points,"[253] "critical Internet resources,"[254] or "points of control"[255] for truly independent expression and activity. No amount of vertical integration can overcome these choke points if certain intermediaries choose to administer critical internet resources in ways that advance ideological goals. Put differently, short of building a separate, entirely self-contained internet, no online rebel can ever be truly full-stack.

While cyberlaw scholarship has long acknowledged these choke points, it has largely focused on the danger that governments might exploit them to censor or surveil citizens.[256] Just as concerning, however, is the growing risk that *private* intermediaries might engage in similar behavior. For most of the internet's history, core infrastructural intermediaries stayed out of the content moderation game, deferring instead to higher-layer providers to figure out how to deal with lawful but awful content. But this forbearance was born of convention, not law. Core infrastructural intermediaries long regarded themselves as mere technical stewards of internet stability and steadfastly resisted calls to expand their narrow, self-defined roles.[257] Although such unwritten rules sufficed for decades to maintain viewpoint neutrality in the core of the internet, those rules may now be unraveling, leading to new forms of content control that require taking a fresh look at interventionist theories.

For example, in November 2018, incels.me was taken offline—its domain name permanently suspended—after it failed to remove user

253. Derek E. Bambauer, *Filtering in Oz: Australia's Foray into Internet Censorship*, 31 U. PA. J. INT'L L. 493, 508 (2009).

254. LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 34 (2014).

255. Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

256. *See, e.g.*, Xueyang Xu, Z. Morley Mao & J. Alex Halderman, *Internet Censorship in China: Where Does the Filtering Occur?*, 6579 PASSIVE & ACTIVE MEASUREMENT 133 (2011) (explaining how Chinese censors place Intrusion Detection System devices within networks to perform keyword filtering); Zittrain, *supra* note 255, at 653 (noting that a Pennsylvania statute requiring ISPs to block access to illegal pornography, if mimicked and expanded, "could become a comprehensive scheme for widespread content control"); Bambauer, *supra* note 253 (describing Australia's "mandatory Internet censorship" program).

257. *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/T324-4MNS] (resisting pressure from various stakeholders to help police blasphemy, hate speech, pornography, and other categories of content that may be illegal in certain countries).

content that allegedly promoted violence.[258] The incels.me suspension was part of a broader emerging movement to suspend or cancel domain names associated with offensive or controversial websites.[259] But whereas other domain takedowns had come at the hands of domain registrars—entities that enable website owners to register domains but that do not play any role in operating the domains—incels.me was targeted by the company responsible for administering the .me top-level domain. As a result, while other victims of DNS takedowns managed to eventually find alternative registrars and get back online, incels.me could, by definition, *never* switch to a different top-level domain. It and its associated website remain offline to this day.

In January 2021, YourT1Wifi, a small Idaho ISP, informed customers that it would block Facebook and Twitter by default.[260] Ostensibly responding to customer demand for such blocking, its actions were clearly intended as a counterstrike against popular social networks for suspending then-President Donald Trump following the January 6th Capitol riot. Although ISPs have, on occasion, blocked access to illegal content,[261] and sometimes even to lawful content for competitive reasons,[262] YourT1Wifi's actions broke new ground in the United States by blocking customers' access to *lawful* content based solely on ideology—namely, the ISP's moral objection to Twitter's and Facebook's content moderation policies.[263] Such actions mimic those of Telus, Canada's second-largest telecommunications company, which was found to have blocked access to a website supporting a labor strike against the company.[264]

Most concerning of all, however, was an event in the Parler saga that received little public attention. While countless articles were written alternately criticizing or defending AWS's decision to terminate cloud

---

258. 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/2NSF-A5GY].

259. *See* Nugent, *supra* note 114, at 72–78.

260. Bode, *supra* note 12.

261. *See* Bill Dedman & Bob Sullivan, *ISPs Are Pressed to Become Child Porn Cops*, NBC NEWS (Oct. 16, 2008, 4:05 AM), https://www.nbcnews.com/id/wbna27198621 [https://perma.cc/K3QE-CBGQ].

262. *See supra* section I.C.2 (describing the efforts of various ISPs to block access to competitive services).

263. Bode, *supra* note 12 (grounding its decision in "a moral high ground of fair and decent communication" (quoting @RightWingCope, TWITTER (Jan. 11, 2021, 9:00 AM), https://twitter.com/RightWingCope/status/1348676046728605700 (last visited Apr. 1, 2023))).

264. *See* Ian Austen, *A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship*, N.Y. TIMES (Aug. 1, 2005), https://www.nytimes.com/2005/08/01/business/worldbusiness/a-canadian-telecoms-labor-dispute-leads-to-blocked.html (last visited Apr. 1, 2023).

hosting services to Parler,[265] less notice was paid to a far more consequential development. After being kicked off AWS, Parler struggled to find another cloud provider willing to endure the public scorn that might result from hosting the controversial social network.[266] Eventually, Parler managed to find a host in DDoS-Guard, a Russian cloud provider that has served as a refuge for other exiled websites, such as 8chan and Daily Stormer.[267] Initially, Parler's flight to DDoS-Guard seemed like a winning move against those who hoped to no-platform the social network. Based in Russia and already willing to host known extremist content, DDoS-Guard would hardly be vulnerable to public shaming campaigns from Western activists. While Parler had not become a true full-stack rebel, it *had* managed to build on top of a couple layers that seemed impervious to deplatforming.

But no degree of control within the topmost layers of the internet stack can escape the choke points located in the lowest layer. And in January 2021, Parler again went offline after the DDoS-Guard IP addresses it relied on were revoked.[268] That revocation came courtesy of Ron Guilmette, a researcher, who, according to one security expert, "has made it something of a personal mission to de-platform conspiracy theorist and far-right groups."[269] In searching for an angle against DDoS-Guard, Guilmette noticed that two thirds of the Russian provider's IP addresses had been allocated by the Latin America and Caribbean Network Information Centre (LACNIC), the regional internet registry responsible for managing IP address space in the Latin American and Caribbean region.[270] Guilmette contacted LACNIC to allege that DDoS-Guard had fraudulently obtained its LACNIC addresses through a Belize-based subsidiary that appeared to have no in-country employees.[271] Shortly thereafter, LACNIC revoked more than eight thousand IP addresses held

265. *Compare* Marni Soupcoff, *Amazon Had Every Right to Stop Hosting Parler*, NAT'L POST (Jan. 14, 2021), https://nationalpost.com/opinion/marni-soupcoff-amazon-had-every-right-to-stop-hosting-parler [https://perma.cc/MC9L-AWN4] (defending), *with* Glenn Greenwald, *How Silicon Valley, in a Show of Monopolistic Force, Destroyed Parler*, SUBSTACK (Jan. 12, 2021), https://greenwald.substack.com/p/how-silicon-valley-in-a-show-of-monopolistic [https://perma.cc/2FHU-G44C] (criticizing).

266. *See* Complaint at 12–13, Parler LLC v. Amazon Web Services, Inc., 514 F.Supp.3d 1261 (W.D. Wash. Jan. 11, 2021) (No. 2:21-cv-00031-BJR) (claiming that "Parler has also been unable to find an alternative web hosting company" because AWS's claims "have made Parler a pariah").

267. Jason Murdock, *What Is DDos-Guard? Parler Website Back Thanks to Russian Tech Company*, NEWSWEEK (Jan. 19, 2021, 5:23 AM), https://www.newsweek.com/ddos-guard-parler-website-back-online-russia-servers-hosting-1562507 [https://perma.cc/ZU2X-HSJH].

268. Krebs, *supra* note 15.

269. *Id.*

270. *Id.*

271. *Id.*

by DDoS-Guard (now valued at nearly half a million dollars),[272] taking down Parler and doubtless many other DDoS-Guard-hosted websites in the process.[273]

Although Parler eventually managed to get back online after DDoS-Guard shifted the social network to other IP addresses it held outside of the LACNIC region, LACNIC's actions presented an existential threat to both DDoS-Guard and Parler. By revoking the IP addresses Parler was using to send and receive web traffic, LACNIC made it not merely difficult but impossible for Parler to stay online unless it could find alternate IP address space. Given Guilmette's express intent to target IP addresses used by controversial websites and the strong implication that LACNIC was motivated by similar concerns, the DDoS-Guard revocation may represent the first known instance of IP-based deplatforming.

The significance of this new form of deep deplatforming cannot be overstated. Ever since the internet was first opened to commercial and non-educational uses, it has operated under an implicit social contract that website operators have the right to accept or reject users as they see fit, but users in turn have the right to set up their own websites if no one else would have them.[274] The penalty for extreme views has been marginalization—being confined to seedy chatrooms or operating lonely websites that few visit or link to—it has not been expulsion from the internet altogether.[275] And while few would mourn the loss of execrable content like that found on 8chan and Daily Stormer, as with all forms of speech control, the primary focus should not be on the particular content removed or the actors silenced but on the machinery that could be used in the future to target other viewpoints or communities.

With these concerns in mind, I now turn to articulating a new theory of interventionism premised on preventing viewpoint foreclosure as well as the five fundamental internet rights that naturally flow from that goal.

---

272. *See Buy IPv4 & ASN*, IPv4.GLOBAL, https://auctions.ipv4.global/ [https://perma.cc/PSA7-QRME] (showing a market price of approximately $51.00 per IP address for blocks of size 8,192).

273. *Id.*

274. *See If the Internet Belongs to Everyone, That Includes Gab*, WASH. POST (Nov. 4, 2018, 7:20 PM), https://www.washingtonpost.com/opinions/if-the-internet-belongs-to-everyone-that-includes-gab/2018/11/04/1ff91c64-de0c-11e8-85df-7a6b4d25cfbb_story.html [https://perma.cc/EG5R-4HW2].

275. Some might object at this point that controversial speakers have long been shut out of other forms of media (e.g., television or radio) or that users who are booted from the internet can always evangelize their views through offline channels (e.g., pamphlets or rallies). I address these objections in section IV.A.

III. THE FIVE INTERNET RIGHTS

In the opening sentence of this Article, I posed the following question: When, if ever, should the law intervene in how private intermediaries moderate lawful online content? After tracing the evolution of content moderation and observing the profound implications of permitting deplatforming to encroach on the core infrastructure of the internet, I believe an answer emerges. At a minimum, the law should ensure that all users have certain basic rights to express their viewpoints on the internet in a lawful manner. This theory of interventionism, which I call Viewpoint Access theory, may be articulated more precisely as follows:

> The law should intervene in the private moderation of lawful content where necessary to prevent viewpoint foreclosure, which occurs when a critical mass of core intermediaries effectively prevent a particular lawfully expressed viewpoint from being published on the internet.

In this Part, I make the case for Viewpoint Access theory by demonstrating how it incorporates the most important principles from the other interventionist theories surveyed in Part I while avoiding their weaknesses. I also explain *how* the law may prevent viewpoint foreclosure by guaranteeing five fundamental internet rights—namely, the rights of connectivity, addressability, nameability, routability, and accessibility. But first, to avoid confusion about what Viewpoint Access theory does and does not hold, it is necessary to define some of the terms used in the above thesis statement and, where important, to defend those definitions.

A. Definitions

As stated above, viewpoint foreclosure occurs when a critical mass of core intermediaries effectively prevent a particular lawfully expressed viewpoint from being published on the internet.

We start with lawful expression. These words capture the fact that the expression itself must not violate laws or commit torts (e.g., defame others or infringe intellectual property). Put differently, the user's speech must be fully protected from government interference under the First Amendment. Thus, simply arguing that the age of consent should be lowered would constitute lawful expression, while displaying child pornography to advance the point would not.[276]

276. Throughout this piece, my focus is on U.S. law and how it should protect the speech of U.S. residents from viewpoint foreclosure at the hands of intermediaries that are subject to U.S. jurisdiction (where such speech is otherwise protected under the First Amendment). I do not propose to enact any kind of global policy—for example, through ICANN or the International Telecommunication

Next, publication. For our purposes, publishing a viewpoint on the internet means maintaining a publicly accessible website that expresses a viewpoint held by the website operator or her end users. But why should viewpoint foreclosure be tied to operating a website? Online expression may take many forms, such as email, WhatsApp, or Zoom—the very same online tools Jane first used to discuss her new philosophy with friends and family before taking to the web. Why index on a technology introduced in 1989 that represents only one type of application within the application layer?

The simple answer is that despite the proliferation of internet-based communication technologies over the last thirty-five years, websites remain the archetypal means for publishing one's opinions online. When a business wishes to advertise its wares, it directs consumers to its website. When an organization wishes to explain its stance on a given issue in a manner that is authoritative, canonical, publicly accessible, and in a medium that it alone controls, it does so on its website. When users wish to share or reference statements belonging to others, they do so by sharing URLs to webpages that contain those statements.

More fully, websites alone combine the following attributes:

- **Control:** Operators alone control what content appears on their websites rather than depending on the good graces of other third-party fora or media in which they might speak.
- **Social Valence:** Society ascribes a weight and legitimacy to webpage expression that it does not ascribe to other online technologies, such as instant messages.
- **Accessibility:** The ubiquity of browsers makes any webpage instantly accessible around the world, in contrast to other technologies, such as desktop or mobile apps, that require interested users to adopt and install new special-purpose access tools.
- **Discoverability:** Consumers can often discover the views held by any person or organization by simply "pulling up" that person's or organization's website; not so for unicast or multicast technologies like Zoom meetings.
- **Authority**: Emails or files passed between users can be modified or falsely attributed, whereas publicly recognized certificates cryptographically attest to the authority and authenticity of webpage content.

Union—that would force foreign actors to abide by U.S. constitutional norms or to respect the five internet rights. That said, to the extent another country also wished to protect its citizens against viewpoint foreclosure at the hands of its local intermediaries, it could use this framework to do so. It would simply substitute its own standards for what constitutes lawful speech under local law.

- **Permanency:** Even open fora may be retired, and ephemeral broadcasts may be lost to time, but speakers can make their content always available on their websites.

If publication on the internet means operating a publicly accessible website, then it follows that a core intermediary is an entity that provides a core internet resource necessary to operate that website. Examples of core internet resources include network access, IP addresses, domain names and domain resolution services, and network backbone services. To be sure, operating a website also requires hardware, networking software, and application software. But for purposes of viewpoint foreclosure, the distinction between these two categories of resources lies in the final element of our test—namely, whether a critical mass of core intermediaries can leverage their control over such resources to effectively prevent a viewpoint from being published on the internet.

For viewpoint foreclosure to occur, it might not suffice for only a single core intermediary to deny service to an unpopular speaker. Enough core intermediaries with control over the same resource or service—a *critical mass*—must each deny service so that the resource is made effectively unavailable to the speaker. Precisely how many intermediaries must deny access to achieve that result depends on the resource. For example, a website operator theoretically needs only a single IP address to remain publicly accessible. Regional internet registries therefore constitute what might be called a *strict class* of core intermediaries—if only a single intermediary breaks ranks from those who refuse service, the website operator can stay online. By contrast, in a *fuzzy class*, a subset of core intermediaries may keep a website offline if the operator cannot practically access the services of substitute intermediaries in the same class. For example, it does not benefit a controversial website operator that a handful of internet service providers scattered throughout the world might be willing to provide her with internet access if the geographical area in which her data center sits is serviced by only three ISPs, none of which will return her calls.

B. Enumerating the Rights

Having defined viewpoint foreclosure in more detail, we now turn to the question of how the law can prevent it. In practical terms, for a person to publish her viewpoints online by operating her own website, she must be able to connect her web server to the broader internet so that users can download data (web content) from it. To connect, she must not only have access to an ISP's physical network; she must also have exclusive use of one or more unique IP addresses to which users can direct their requests. Next, to have any realistic hope of bringing human visitors to her website,

she must have exclusive use of a domain name and must benefit from stable DNS resolution services. But mere internet access, which can be provided by a single ISP, is not enough. She must be able to send her web content beyond her ISP's network to the networks used by requesting users, traversing through any intervening networks along the way. Finally, it will do little good that her web content can reach a requesting user's network if that user's ISP can prevent its subscribers from accessing the website, and so end users must also not be blocked.[277]

Accordingly, if we start with the premise that all users should be protected from viewpoint foreclosure, then the law can accomplish this goal by guaranteeing five fundamental internet rights: connectivity, addressability, nameability, routability, and accessibility. I will now describe each of these rights more fully with reference to internet architecture and our running case study.

1. Connectivity

Connectivity means that a website operator can connect to the broader internet.

Typically, a website operator obtains internet access service from an ISP. Thus, Jane, our radical, fictional protagonist, might run her controversial website out of her data center, which could be as complex as a multi-cluster server farm in a temperature-controlled facility or as simple as a laptop in a coat closet. Lacking direct access to her end users' networks, Jane must rely on a commercial ISP, such as Century Link or Verizon Business, to gain indirect access to theoretically all other public networks.

As noted above, connectivity providers constitute a fuzzy class of core intermediaries. If each ISP that services Jane's area refuses to do business with her, she cannot make her website publicly available. Even if the FCC were to reinstate net neutrality rules, such rules would not help Jane for two reasons.

First, net neutrality rules were directed to accessibility rather than connectivity. They aimed to protect subscribers who already *had* internet service by preventing ISPs from blocking their access to lawful websites

277. Although this point should be implicit throughout the Article, these rights are best understood as negative rather than positive rights. The law need not guarantee commercial internet access itself to every user who desires it (e.g., by subsidizing the service for users who can't afford it). Rather, if a user can already afford commercial internet access, domain names, IP addresses, etc., then the law should prevent core intermediaries from *discriminating* against otherwise qualified users based on ideology. *See infra* section III.C.1 (comparing viewpoint access rules to antidiscrimination laws that protect otherwise qualified job applicants); section IV.B (assuming a user with "reasonable financial means").

or services.[278] To use the language of common carriage, net neutrality rules do not include a duty to serve.

Second, by its terms, the 2015 Open Internet Order protected only "mass market" (e.g., residential) subscribers—here, Jane's end users—and therefore limited its scope to last-mile access networks.[279] The 2015 order expressly exempted so-called "edge providers" (such as website operators) and the commercial internet access services they rely on to get online.[280] While residential subscribers could theoretically use their residential internet connection to host a website (in an effort to slot in under potential future net neutrality regulations), many residential ISPs do not allow subscribers to use their services to host websites.[281] And in any event, residential ISP services are not technically well-suited to website hosting.[282]

Colocation (colo) could provide a geographical workaround if no ISPs in Jane's area will serve her but only if other parties play ball. A colo facility operator must agree to house Jane's servers, and even then, other network operators must agree to peer with Jane if she wants to secure a place on the internet. Here too net neutrality offers no assistance. As with its 2010 predecessor, the 2015 Open Internet Order expressly declined to regulate the internet peering or backbone markets.[283]

Accordingly, if we wish to avoid the possibility that lawful websites could be kept off the internet because no private company in the area will provide suitable internet access for offending edge providers, the law must recognize a fundamental right to internet connectivity. That right must guarantee non-discriminatory access to the services of commercial ISPs, which are the only suitable providers for stable websites, and it should ideally extend to the services of colo facility operators as well.[284]

2. Addressability

Addressability refers to the right of a website operator to hold and use static IP addresses.

---

278. *See* 2015 Open Internet Order, *supra* note 198, ¶¶ 14–18 (establishing bright line rules protecting consumers' ability to "access" lawful content).

279. *Id.* ¶¶ 25, 189, 282.

280. *Id.* ¶¶ 195, 203, 205.

281. *See* Cameron Summerson, *Can You Host a Web Server on Your Home Internet Connection?*, HOW-TO GEEK (Sept. 13, 2018, 8:56 PM), https://www.howtogeek.com/362602/can-you-host-a-web-server-on-your-home-internet-connection/ [https://perma.cc/Z4WU-NBEY].

282. *Id.*

283. *See* 2015 Open Internet Order, *supra* note 198, ¶¶ 185, 190, 193–206.

284. *Cf.* Colin Crawford, *Defining a Right to Internet Access Through Public Accommodation Law*, 76 TEMP. L. REV. 225 (2003).

Each device that connects to the public internet uses an IP address, a number that uniquely identifies the device when it comes to sending or receiving communications.[285] Most of the world still relies on Version 4 of the Internet Protocol (IPv4), which specifies a 32-bit address format for a total possible address space of 2^{32} or around 4.3 billion addresses.[286] When it became clear that enough devices would eventually connect to the internet to exhaust IPv4's supply of addresses, Internet Protocol Version 6 (IPv6) was devised to provide a 128-bit address format.[287] Although IPv6 offers an astronomical 2^{128} (or 340 undecillion) unique addresses—enough to assign 100 distinct addresses to every atom on the surface of the earth—the global effort to migrate to IPv6 remains hopelessly stalled.[288] As the world began running out of IPv4 addresses, a secondary market emerged in which private parties could buy and sell address blocks as the only practical way to obtain additional address space.[289] At the time of this writing, the market rate for a block of 256 addresses (the smallest permitted unit of aggregation on the internet) starts at $10,496, a price of $41 per individual address.[290]

IP address administration ultimately rolls up to the Internet Corporation for Assigned Names and Numbers (ICANN). A private, non-profit entity based in California, ICANN is responsible for managing both the domain name space (names) and network identifiers and IP addresses (numbers).[291] In turn, ICANN has delegated responsibility for managing the world's IP addresses to five regional internet registries (RIRs): RIPE (responsible for Europe and the Middle East), APNIC (Australia and much of Asia), ARIN (the English-speaking parts of North America and the Caribbean), LACNIC (South America and the rest of North America),

---

285. Network Address Translation (NAT) and other proxy technologies qualify this statement to some degree, but they do not change the fact that a public IP address (by at least one participating device) is always ultimately necessary for internet communications.

286. Josh Fruhlinger, *What Is IPv6, and Why Is Adoption Taking So Long?*, NETWORK WORLD (Mar. 21, 2022, 3:00 AM), https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html [https://perma.cc/9RMS-KPGU].

287. *Id.*

288. *See* BRENDEN KUERBIS & MILTON MUELLER, INTERNET GOVERNANCE PROJECT, GA. INST. OF TECH., THE HIDDEN STANDARDS WAR: ECONOMIC FACTORS AFFECTING IPV6 DEPLOYMENT 36–39 (2019), https://www.internetgovernance.org/wp-content/uploads/IPv6-Migration-Study-final-report.pdf [https://perma.cc/XF7U-L338] (predicting a continued hybrid IPv4-IPv6 world for at least the next twenty years).

289. *See* Geoff Huston, *The Formation of IPv4 Address Markets*, CIRCLEID (Dec. 16, 2021), https://circleid.com/posts/20211216-the-formation-of-ipv4-address-markets [https://perma.cc/EE5T-KU63].

290. *See* IPv4.GLOBAL, *supra* note 272.

291. *What Does ICANN Do?*, ICANN, https://www.icann.org/resources/pages/what-2012-02-25-en [https://perma.cc/J9JE-8VE5].

and AfriNIC (Africa).[292]

Although IP addresses are critical internet resources, RIRs have largely stayed out of the content moderation game for at least two reasons.

First, RIRs have only blunt tools to discipline website operators. Currently, the smallest amount of address space that can be allocated by any RIR is a block of 256 sequential addresses. Therefore, if an RIR wished to prevent a controversial website from using even a single IP address, the RIR could do so only by revoking an entire 256-address block (or an even larger block). Doing so could take down other innocent websites that use other addresses within the block. But such bluntness could also operate as an advantage. If the website is hosted by another provider, such as a cloud provider, threatening to revoke the provider's address space—and, thus, harm more of its customers—unless the provider excises the offending website would act as a powerful incentive.[293]

Second, RIRs have historically resisted calls from governments and others to police behavior on the internet, including even illegal behavior. ARIN's Registration Services Agreement even states that "ARIN does not have the ability to control or influence content accessible through [IP addresses] from ARIN."[294] However, this provision states only what ARIN alleges that it can or cannot do. It stops short of *committing* not to use its power over IP addresses or network numbers to control content.[295] And, notably, no other RIRs have followed ARIN's lead in this regard or committed not to attempt to influence content.

In fact, all five RIRs reserve the right to revoke address space in certain circumstances. Reasons include if an address holder fails to announce allocated addresses to neighboring networks within 90 days (LACNIC),[296]

---

292. DEEP MEDHI & KARTHIK RAMASAMY, NETWORK ROUTING: ALGORITHMS, PROTOCOLS, AND ARCHITECTURES § 10.3 (2d ed. 2018).

293. If a full-stack rebel operates its own network (autonomous system), a more surgical strike would be for an RIR to simply revoke the associated autonomous system number (ASN).

294. AM. REGISTRY FOR INTERNET NOS., LTD., REGISTRATION SERVICES AGREEMENT VERSION 13.0 § 2(f) (2022) [hereinafter ARIN RSA], https://www.arin.net/about/corporate/agreements/rsa.pdf [https://perma.cc/7H6H-RDQD].

295. To be clear, ARIN's policies do not currently provide for content control. *See Number Resource Policy Manual*, ARIN (Mar. 1, 2023), https://www.arin.net/participate/policy/nrpm/ [https://perma.cc/8QT4-9S89]. And any change to ARIN policies would need to go through a public policy development process and be approved by ARIN's Board of Trustees, which is elected by ARIN's members (address-holders). *See Policy Development Process (PDP)*, ARIN (Jan. 14, 2013), https://www.arin.net/participate/policy/pdp/ [https://perma.cc/BP73-UB9J]. However, provided that ARIN's Policy Development Process is followed, ARIN, like other regional internet registries, is relatively unconstrained in terms of the policies it may enact or repeal.

296. LATIN AM. & CARIBBEAN NETWORK INFO. CTR., LACNIC POLICY MANUAL VERSION 2.15

provides incorrect registration information or fails to keep such information up to date (APNIC),[297] violates any applicable laws (AfriNIC),[298] fails to adequately respond to requests for information (ARIN),[299] or simply acts in a way that "cause[s] damage to the name" of the RIR (RIPE).[300] While it might be straightforward to comply with some of these requirements, prohibiting address holders from damaging the name of RIPE would seem to leave RIPE with wide discretion to revoke IP addresses used by a controversial website if public sentiment turned against RIPE for its role in keeping the website online. Requiring address holders to comply with applicable law could provide another hook for IP-based deplatforming, since offensive speech on a globally available website could easily violate the laws of countries that take a narrower view of free expression than does the United States. And in any event, all five RIRs reserve the right to update their terms of service,[301] thus providing no guarantees against future content controls.

Moreover, because much of the world's address space was allocated before RIRs were even formed, it is well known that RIR registries are hopelessly inaccurate and that their policies are only loosely enforced.[302] Vast swaths of address space are currently used by network operators whose information is either inaccurate or wholly absent from registry databases.[303] Foreign entities routinely establish local subsidiaries to obtain address space in RIR regions. And requirements that IP addresses be used primarily within the issuing RIR's region are routinely ignored.

As such, if an RIR wished to target a particular address holder, it would not be difficult for the RIR to find at least one technical policy violation.

---

§§ 1.11, 7 (May 19, 2022) [hereinafter LACNIC POLICY MANUAL], https://www.lacnic.net/innovaportal/file/680/1/manual-politicas-en-2-15.pdf [https://perma.cc/YYR3-RDWX].

297. *Membership Agreement: Member's Obligations*, APNIC (Feb. 9, 2012), https://www.apnic.net/about-apnic/corporate-documents/documents/membership/membership-agreement/ [https://perma.cc/Z7UD-QJJF].

298. AFR. NETWORK INFO. CTR., AFRICAN NETWORK INFORMATION REGISTRATION SERVICE AGREEMENT § 4(c)(ii)(2) (Nov. 27, 2017), https://afrinic.net/ast/pdf/services/afrinic-rsa-en-201801.pdf [https://perma.cc/RK5F-FPDD].

299. ARIN RSA, *supra* note 294, §§ 2(c), 13(b).

300. *Standard Service Agreement: Art. 9.4*, RIPE NCC (June 9, 2020), https://www.ripe.net/publications/docs/ripe-745 [https://perma.cc/97SY-V9LN].

301. *See, e.g.*, ARIN RSA, *supra* note 294, § 1(d) ("ARIN reserves the right, in its sole and absolute discretion, to amend, supplement, restate or otherwise modify any or all Policies at any time.").

302. *See* Edvinas Račkauskas, *IP Legacy Space Explained*, IPXO (Dec. 31, 2021), https://www.ipxo.com/tutorial/ip-legacy-space/ (last visited May 12, 2023).

303. *Id.* ("According to ARIN, 53% out of the roughly 25,000 legacy networks registered in ARIN's Whois have either no associated Point of Contact (POC) or have a POC that has never been verified by ARIN (referred to as an Invalid POC).").

In the case of Parler, IP addresses held by DDoS-Guard were revoked based on section 1.14 of the LACNIC Policy Manual, which requires address holders to be located within the LACNIC service region (South and Central America).[304] Yet DDoS-Guard *did* appear to meet the letter of the law by maintaining a Belizean subsidiary, even if no employees worked in Belize (which is not required by the rule). It could be that DDoS-Guard failed to comply with LACNIC's requirement that an address holder provide services primarily within the LACNIC region.[305] But no reporting has identified this provision as a basis for LACNIC's decision, and, as stated above, such requirements are widely disregarded. These facts, coupled with the involvement of Ron Guilmette, a committed ideological deplatformer, raise the likelihood that LACNIC targeted DDoS-Guard and the controversial websites it hosted based on their viewpoint.

Relatedly, following Russia's invasion of Ukraine, Ukraine's Deputy Prime Minister sent a letter asking RIPE to revoke Russia's existing IPv4 and IPv6 addresses because Russia was using some of them to host "websites continuously spreading disinformation, hate speech, promoting violence and hiding the truth regarding the war in Ukraine."[306] Although RIPE rejected Ukraine's request, and although the five internet rights would pertain only to users in the United States, the fact that the request was made in the first place shows that IP-based takedowns are increasingly entering the public consciousness as a potential weapon of ideological warfare, if not actual warfare.

Therefore, given the crucial role of IP addresses in communicating online, the law should grant website operators a fundamental right to IP address space lawfully held and used, including basic property and non-discrimination protections.

3. Nameability

Nameability refers to the right of a website operator to maintain a domain name and, when users query the domain name, to have those queries answered (resolved) by returning the IP address at which the website is hosted.

As the authority for the domain name space, ICANN delegates each

304. Krebs, *supra* note 15; *see also* LACNIC POLICY MANUAL, *supra* note 296, § 1.14 ("The numbering resources under the stewardship of LACNIC must be distributed among organizations legally constituted within its service region . . . and mainly[] serving networks and services operating in this region.").

305. LACNIC POLICY MANUAL, *supra* note 296, § 1.14.

306. *See* Federov Letter, *supra* note 16.

top-level domain (e.g., .edu) to a single registry operator.[307] In turn, each registry operator maintains an authoritative registry indicating which entities have exclusive rights to which second-level domains (e.g., princeton) within their top-level domains.

While some registry operators interface directly with customers that register individual domain names, most do not. Instead, to register radicaljane.chat as her domain name, Jane must engage an ICANN-accredited registrar, such as GoDaddy. The registrar (GoDaddy) charges the registrant (Jane) a registration fee and instructs the operator of the top-level domain to update its registry to reflect the fact that Jane now has exclusive rights to the domain.

But merely registering a domain name does not make it operational. When users type a domain name into their browsers (or click a link), the result is that a DNS query is sent to the registry operator, which must respond with authoritative IP address information associated with the domain name. If that process (called DNS resolution) is not performed, the domain name is as good as useless.

This description reveals two choke points in the DNS. First, for a website operator to maintain a domain name, she must be able to register and maintain her registration in the applicable registry database. Second, user queries to the domain name must be resolved. While the registry operator alone controls the second choke point, registrars play a role in the first. As briefly touched upon in section II.C., registrars have increasingly waded into the content moderation game through "morality clauses" in their terms of service. For example, registrars have prohibited registrants from associating domain names with websites that host "'profane,' 'vulgar[],' 'embarrass[ing],' 'derogatory,' 'racist,' 'homophobic,' . . . 'blasphemous,'" or other "morally objectionable" content.[308] Thus, dailystormer.com, gab.com, ar15.com, and other

307. This paragraph and the next draw heavily from Nugent, *supra* note 114, at 49–62.

308. Nugent, *supra* note 114, at 74 (first quoting *Terms and Conditions: Representations and Warranties*, INTERNET.BS (Nov. 14, 2019), https://internetbs.net/en/domain-name-registrations/termsandconditions.html [https://perma.cc/Z99T-M7D5]; then quoting *Dynadot Service Agreement, Version 3.5.76: Disputes*, DYNADOT (May 15, 2019), https://www.dynadot.com/registrationagreement.html [https://perma.cc/SQ9D-MNN9]; then quoting *Annulet Incorporated Terms and Services Agreement: Proper Use Policy*, ANNULET, https://www.annulet.com/#/content/18 [https://perma.cc/48DG-2TFQ]; then quoting *General Terms and Conditions, Version 2.2014: Abuse; Notice and Takedown; UDRP*, REALTIME REGISTER, https://www.realtimeregister.com/resources/terms-conditions/ [https://perma.cc/6DUA-TCBL]; then quoting *Register.it General Conditions of Service: Use of the Services and Customer Liability*, REGISTER.IT (May 8, 2020), https://www.register.it/company/legal/condizioni-generali.html?lang=en [https://perma.cc/GW6Z-WQHB]; and then quoting *Domain Name Registration Services: Registrant Responsibilities*, WEB.COM (Sept. 7, 2017),

websites have seen their domain names suspended simply because their registrars disliked their viewpoints.[309]

Of course, registrars constitute a strict class of core intermediaries. Jane need find only a single amoral registrar to avoid DNS-based deplatforming. And registrants can usually escape censorious registrars by transferring their domain names to other registrars[310] (unless a registrar decides to go nuclear by canceling rather than suspending a domain name). Short of that, Jane could even set up shop as her *own* registrar and thereby get direct access to underlying top-level registries. But if the registry operator itself refuses to register or perform resolution services for Jane's controversial domain, she has few remaining options. She cannot transfer radicaljane.chat to another registry operator, since only one operator controls each top-level domain. She could potentially register in a different top-level domain (e.g., radicaljane.net), but that would force her to abandon her original domain name altogether, a move that can be fatal for a website. Such was the case for incels.me, when the .me registry operator permanently suspended the domain name in 2018.[311]

Registry operators, too, form a strict class of core intermediaries, and if a beleaguered website operator is willing to abandon her domain name for another, she need find only a single top-level domain operator that will register and service her domain name—e.g., radicaljane.ru (Russia) as a last resort.

But the prospect of top-down content control in the DNS may not be far away. Because ICANN has final authority over registry and registrar operations, it could be said that ICANN represents a core intermediary class of only one. Already, ICANN is wading into content moderation by requiring entities that administer new top-level domains to enforce certain content controls.[312] Or ICANN could bypass registry operators altogether by requiring registrars to reject "abusive" domain names as a condition to remaining accredited.[313]

But even if ICANN does not elect to use its power over the DNS to control content, given the centrality of domain names to operating

---

https://assets.web.com/legal/English/DomainNameRegistrationServices.pdf [https://perma.cc/6LBL-BBDW]).

309. Nugent, *supra* note 114, at 78; Bode, *supra* note 12.

310. *Transfer Policy*, ICANN, https://www.icann.org/resources/pages/transfer-policy-2016-06-01-en [https://perma.cc/KD3Q-6D3P].

311. *See* Nugent, *supra* note 114, at 87.

312. *See id.* at 77–78.

313. *Id.* at 79 (quoting Caroline Bricteux, *Regulating Online Content Through the Internet Architecture: The Case of ICANN's New gTLDs*, 7 J. INTELL. PROP., INFO. TECH. & ELEC. COM. L. 229, 244 (2016)).

publicly accessible websites, the law should step in to prevent DNS administration from becoming just another lever in the culture war by guaranteeing a right to nameability.[314]

4. Routability

Routability refers to the right of a website operator to have traffic to and from her website faithfully routed between intervening networks.

The term internet—short for "inter-network"—concisely captures the fact that the internet operates as a network of networks (in technical parlance, *autonomous systems*). Users and providers typically connect to *access networks* provided by ISPs, such as Comcast or T-Mobile, which promise to connect subscribers to the broader internet (i.e., to other networks). To fulfill that promise, ISPs both peer (connect) directly with each other, where possible, and purchase long-haul transit services from providers that operate *backbone networks* (also called *core networks*) in order to reach other networks with which they cannot peer.[315]

Internet communication, therefore, is fundamentally a matter of "hopping" across networks, where each intervening network represents an additional hop between source and destination. Each network learns where to route internet traffic by receiving information from border routers in neighboring networks that "announce" which IP addresses they own and which other networks they can reach. Given the web-like nature of the internet, where each network might interconnect with one or more other networks, a communication may be routed from a source device to a destination device using multiple paths. For example, as depicted in Figure 6, Vikram, an avid reader of Jane's blog, might connect to Jane's

---

314. Of course, such a right to nameability need not extend to every top-level domain. Some top-level domains were delegated with the expectation (or requirement) that only certain types of entities or websites would be able to register domain names. Examples include commercial top-level domains (e.g., .bmw), country code top-level domains with regionality requirements (e.g., .ca), and special interest top-level domains (e.g., .lgbt). *See What Is a Restricted TLD?*, DYNADOT, https://www.dynadot.com/community/help/question/what-is-restricted-tld [https://perma.cc/A968-DDUG]. It might therefore be sufficient if the nameability right were limited to a handful of general-purpose top-level domains, such as .com, .org, and .net. Fortunately, as part of its Cooperative Agreement with Verisign to operate the internet's authoritative root zone file, the NTIA currently requires Verisign to operate the .com registry in a content-neutral manner. *See* NAT'L TELECOMMS. & INFO ADMIN., U.S. DEP'T OF COM., COOPERATIVE AGREEMENT NO. NCR-92-18742, AMENDMENT TO FINANCIAL ASSISTANCE AWARD No. 35 (2018), https://www.ntia.doc.gov/files/ntia/publications/amendment_35.pdf [https://perma.cc/W3FU-YHCB] ("Verisign will operate the .com registry in a content neutral manner and . . . participate in ICANN processes that promote the development of content neutral policies for the operation of the DNS."). A proper right to nameability would see this contractual provision (which could be dropped at any time) enshrined in the law.

315. 2015 Open Internet Order, *supra* note 198, ¶ 196–98.

webserver through a path that traverses the T-Mobile → Century Link → Verizon Business networks (two hops) or the T-Mobile → NTT → Comcast → Verizon networks (three hops).

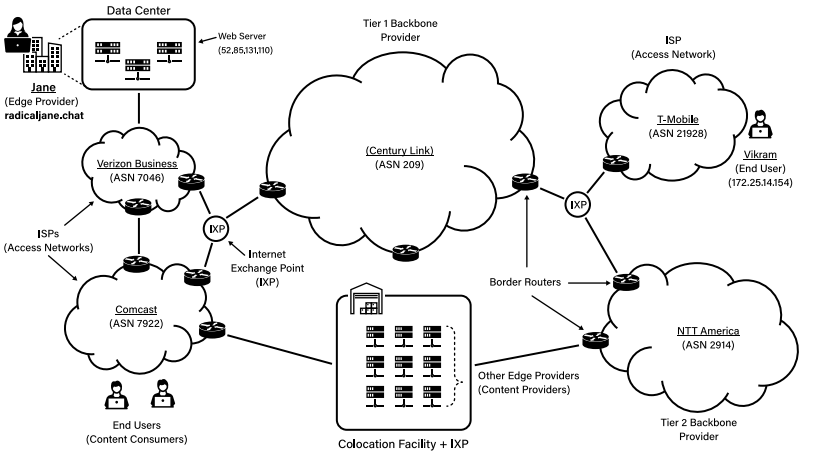

Figure 6 – Internet Routing

This ability to dynamically route traffic via different combinations of independently operated networks was one of the great innovations of the internet. In contrast to predecessor telephone networks, in which two devices might connect via only a single, vulnerable path, the multi-network nature of routing makes the internet highly resilient. Should a router, link, or even an entire network go down, internet traffic can often find another route, however convoluted, to reach its destination, just as water seeks its own level. Nor is resiliency limited to evading network outages. Legal or geopolitical considerations, or even the desire to remain undetected, may motivate internet actors to choose one route over another. As John Gilmore, founder of the cyber-libertarian Electronic Frontier Foundation, famously proclaimed, "[t]he Net interprets censorship as damage and routes around it."[316]

But this architecture, which relies on trust, also makes the internet insecure. Occasionally, networks inadvertently announce address blocks they don't own, creating routing conflicts. A bad actor can attempt to steal traffic intended for another network or block users from accessing the latter's content by deliberately announcing that other network's addresses

316. Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME (Dec. 6, 1993), https://content.time.com/time/subscriber/article/0,33009,979768,00.html [https://perma.cc/SZ9M-XNEL].

as its own, a technique known as "BGP hijacking."[317] In 2008, for example, a state-controlled network operator in Pakistan falsely announced certain address blocks belonging to Google in an effort to prevent users in Pakistan from accessing YouTube. However, because other networks outside of Pakistan peered with the Pakistani operator and honored the operator's false announcements, the routing lie propagated to networks in other countries, causing YouTube to become unreachable for a substantial percentage of the world's internet users.[318]

Such techniques could be used by network operators or others to take down unpopular websites by BGP hijacking. Or, less dramatically, network operators could simply refuse to route traffic to or from an unpopular website by declining to announce the website's addresses or network number to neighboring networks. For example, after Cloud Innovation, an English colo provider, made itself a pariah in the African community by suing AfriNIC, several African ISPs publicly discussed ceasing to route packets to IP addresses belonging to the company as a form of ideological retribution.[319]

A backbone network operator that took this approach would not necessarily *block* traffic to or from the site, but it would remove itself as a potential hop for any network traffic addressed to the site.[320] And if enough backbone networks did likewise, a website could become effectively unreachable for large swaths of users. Thus, if Vikram tried to access Jane's website, T-Mobile's routers might have no way of reaching Jane's network, since none of its peers would claim to know how to reach Jane's IP addresses or her network.

Of course, market forces currently discourage such behavior. Network operators that peer with other networks want to see their routing

---

317. *See* Shinyoung Cho, Romain Fontugne, Kenjiro Cho, Alberto Dainotti & Phillipa Gill, *BGP Hijacking Classification*, *in* NETWORK TRAFFIC MEASUREMENT AND ANALYSIS CONFERENCE 2019 25, 25 (2019). BGP stands for Border Gateway Protocol, which is the protocol networks use to advertise which IP address ranges they own and therefore which communications should be routed to them.

318. Declan McCullagh, *How Pakistan Knocked YouTube Offline (and How to Make Sure It Never Happens Again)*, CNET (Feb. 25, 2008, 4:28 PM), https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/ [https://perma.cc/S4KN-NWNW].

319. *See* Milton Mueller, Vagisha Srivastava & Brenden Kuerbis, *A Fight Over Crumbs: The AFRINIC Crisis*, INTERNET GOVERNANCE PROJECT (Aug. 19, 2021), https://www.internetgovernance.org/2021/08/19/a-fight-over-crumbs-the-afrinic-crisis/ [https://perma.cc/9K6X-M92P].

320. *See* MILTON MUELLER, WILL THE INTERNET FRAGMENT 24 (2017) ("[N]othing compels any single Autonomous System (APs) to open itself up completely to all others. All APs can exercise . . . control over who they interconnect with, what packets they admit into or out of their systems, what services they want to accept or block, [and] what content can enter and leave.").

announcements faithfully and accurately propagated. Some peering agreements may even require it.

But it cannot be ignored that, like other core intermediaries, backbone providers have the power to effectively take down website content by refusing to relay traffic to and from offensive websites. Any theory of interventionism premised on preventing viewpoint foreclosure should therefore take account of a right to routability.

5. Accessibility

Finally, accessibility refers to the right of a website operator not to have users blocked from accessing her website.

The accessibility right is similar to the routability right in that it protects the flow of traffic to and from a website, but it differs in its focus. Whereas the routability right focuses on backbone networks that serve to bridge other networks, the accessibility right focuses on the final hop in the transmission process—namely, the access networks end users use to find and access content on the internet.

This distinction is important. A single backbone network generally cannot prevent users from accessing a website; it can only refuse to act as a networking hop for traffic to and from the website. By contrast, because subscribers rely on their access networks to reach all other networks on the internet, an access network operator (an ISP) can effectively block the website for *all* its subscribers. In telecom jargon, an ISP possesses a "terminating access monopoly" to its subscribers.[321] As depicted in Figure 6, Vikram (an end user) might rely on T-Mobile to connect to the internet, but since Vikram is not directly connected to any other networks, T-Mobile can effectively prevent him from reaching any website it chooses.

Some ISPs already block access to illegal or infringing websites.[322] Although the federal Stop Online Privacy Act (SOPA)[323] and PROTECT IP Act (PIPA) bills,[324] which would have required ISPs to block certain

---

321. Jonathan E. Nuechterlein & Christopher S. Yoo, *A Market-Oriented Analysis of the "Terminating Access Monopoly" Concept*, 14 COLO. TECH. L.J. 21, 35 (2015).

322. *See, e.g.*, Jon Brodkin, *Every ISP in the US Has Been Ordered to Block Three Pirate Streaming Services*, ARS TECHNICA (May 3, 2022), https://arstechnica.com/tech-policy/2022/05/judge-rules-every-isp-in-us-must-block-pirate-sites-run-by-mysterious-defendants/ [https://perma.cc/3M7X-YZ46] (describing a court ruling requiring ninety-six ISPs to block three copyright-infringing websites); Robert Smith, *Internet Providers Agree to Block Child Porn Sites*, NPR (June 10, 2008, 6:05 PM), https://www.npr.org/2008/06/10/91366026/internet-providers-agree-to-block-child-porn-sites [https://perma.cc/XH9B-Q5BB] (describing an agreement by Verizon, Sprint, and Time Warner Cable to block child pornography at the urging of the New York Attorney General).

323. Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

324. PROTECT IP Act, S. 968, 112th Cong. (2011).

infringing sites, met an ignominious end after a well-publicized online revolt, copyright holders are nonetheless securing similar injunctions from courts.[325]

But ISPs have just as much power to block *lawful* websites as they do unlawful websites. Thus, even if Jane migrates her radical (though lawful) website to foreign servers to better control her technical destiny, a very public deplatforming campaign could attempt to pressure U.S.-based ISPs to block users in the United States from accessing Jane's offshore-hosted website.

Such actions would no doubt violate net neutrality rules were they still in effect. Each of the FCC's three attempts at net neutrality included some form of a no-blocking rule that prevented certain ISPs from blocking subscribers' access to lawful applications and websites.[326] And California's Internet Consumer Protection and Net Neutrality Act,[327] which the state enacted in 2018 after the demise of federal net neutrality rules, currently prohibits such behavior.[328] But as described in Part I, net neutrality has historically targeted *economic* discrimination, not moral or ideological discrimination.[329] It aimed to prevent ISPs from leveraging their power over their own networks to block subscribers from accessing websites either because the ISP offered a competing product or because the ISP wished to extract a toll from website operators to reach its subscribers.

Of course, taken literally, net neutrality rules would prevent ISPs from blocking *any* lawful website, regardless of the reason (economic or moral). But it remains to be seen whether net neutrality advocates, who tend to populate the political left, will continue to support such broad rules if those on the political right begin attempting to use them to protect far-right websites from left-led deplatforming campaigns.

C. A New Theory of Interventionism

Having enumerated the five internet rights, I'll now explain why Viewpoint Access theory provides a superior basis for interventionism. As I'll show, Viewpoint Access theory addresses each of the core concerns raised by existing user-centric theories, but it does so while

---

325. *See* Annemarie Bridy, *Three Notice Failures in Copyright Law*, 96 B.U. L. REV. 777, 825–29 (2016).

326. *See* 2015 Open Internet Order, *supra* note 198, ¶¶ 111–18; *supra* text accompanying notes 197–201.

327. CAL. CIV. CODE §§ 3100–3104 (West 2018).

328. *Id*. § 3101(a)(1).

329. *See supra* section I.C.2.

respecting the countervailing values that animate provider-centric theories.

1. Viewpoint Access Theory and User-Centric Principles

Viewpoint Access theory—which protects the right to express a viewpoint on the internet in a lawful manner by maintaining a publicly accessible website—is consistent with the most important principles captured in each of the user-centric theories canvassed in Part I: Expressive Rights, Non-Discrimination, and User Property Rights.

Expressive Rights. With respect to users' expressive rights, Viewpoint Access theory certainly aligns with the major rationales underlying the First Amendment, as I'll demonstrate shortly. But does the First Amendment itself *require* basic viewpoint access?

While arguments for classifying higher-layer providers, such as social media companies, as state actors are quite weak, it's worth exploring whether a stronger case could be made for core intermediaries. As explained above, social media companies do not qualify as state actors because they do not perform functions historically and exclusively performed by the state. This same deficiency likewise dooms any efforts to classify mid-stack intermediaries, such as cloud providers and software vendors, as state actors. But are core intermediaries any different?

They might be if we look not at their function but at their effect. Users deplatformed from this or that social media site can likely find a substitute or, at the very least, create their own website. But users targeted by core intermediaries can be removed from the internet altogether and thereby removed from today's public square. To be sure, those banished from the internet can still access *literal* public squares. Exiled users can still picket on physical sidewalks, and deplatformed political groups can hold rallies in public parks. But it was also true that religious minorities remained free to distribute leaflets on streets outside of Chickasaw, Alabama.

One way of interpreting the concern animating the *Marsh* Court is that private parties might so thoroughly replicate and displace traditional public spaces that, having drawn public activities completely onto private property, owners could then shut down those activities they disapproved of, including constitutionally protected speech and religious exercise. While critics of *Marsh* could quibble about this or that doctrine of property law, if one simply steps back to look at the broader picture, it seems hard to defend the proposition that if certain Chickasaw residents wanted to exercise their constitutional rights, they just had to move to another town.

The same is true of the internet. Just as the state of Alabama ceded operation of Chickasaw to a private corporation, the federal government

incrementally handed over control of the public internet to private parties until no public cyberspace remained.[330] As a result, individuals now use the internet solely at the pleasure of private entities that can proscribe constitutionally protected speech and, similar to the Gulf Shipbuilding Corporation in *Marsh*, literally prosecute non-compliant users for trespass.[331] While users remain free to express themselves offline, we should once again take a step back to ask whether it's any easier to defend the proposition that if certain users want to exercise their constitutional rights, they just have to leave the internet.[332]

Short of constitutionally based strong interventionism, however, Viewpoint Access theory sufficiently aligns with the major rationales underlying the First Amendment discussed in Part I to merit at least the weak interventionism of targeted legislation.

While it might not advance the search for truth to permit every troll to post on Reddit to his heart's content, it seems self-evident that permitting private parties to banish disfavored viewpoints from the internet altogether would hinder the search. As described above, the lab leak theory (a particular viewpoint) was banned from major social media platforms as an outlandish (and possibly dangerous) conspiracy theory.[333] That viewpoint was eventually welcomed back to the major platforms not because platform operators simply changed their minds but because a growing body of evidence supporting the theory accumulated elsewhere on the internet—in niche media sites, blogs, and personal websites. Those off-platform properties were less powerful tools for evangelizing the theory, but because they were online properties, they were able to leverage the generative power of the web to facilitate collaboration and crowdsourcing,[334] which in turn enabled the theory to eventually achieve critical mass.

This dynamic describes the opportunity space for any viewpoint expressed online. Those views excluded from major platforms must find a home in the backwaters of the internet. The less reputable or plausible an opinion, the more obscure the sites it must depend on to stay online. But implicit in this sliding scale is the promise that as long as an idea can

---

330. *See* ROXANA RADU, NEGOTIATING INTERNET GOVERNANCE 75–112 (2019) (chronicling the privatization of the public internet).

331. *See* 18 U.S.C. §§ 1030(a)(2), (c) (criminalizing the act of intentionally accessing a computer without authorization).

332. *Cf.* Aswad, *supra* note 53, at 31 ("[H]ow much will it matter ten or fifteen years from now that the First Amendment (and international human rights law) protect freedom of expression, if most communication happens online and is regulated by private platforms that do not—and are not required to—adhere to such long standing substantive norms on expression?").

333. *See supra* section I.C.1.

334. *See generally* Jonathan Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006).

plant itself in some parcel of cyberspace, it can potentially grow and spread to other parcels. In time, it may even win over respectable institutions and graduate to the big leagues of the major platforms. But this hope of future vindication, however slim, is not available to viewpoints that are prevented from germinating in even the humble grounds of self-hosted websites. Such viewpoints are denied the opportunity to be discovered online, where they can be considered, critiqued, and potentially improved upon. The phenomenon of viewpoint foreclosure, therefore, hinders the search for truth, impoverishing public discourse by stamping out heterodox ideas that may contain important kernels of truth.

That impoverishment can also have consequences beyond scientific and cultural debates. Where viewpoints touch upon matters of electoral importance, foreclosure can harm the enterprise of self-government. Deprived of perspectives that might influence their votes, citizens will be less informed, and electoral outcomes may be altered. Of course, electoral outcomes may also be skewed by misinformation and toxic rhetoric that is allowed to remain online. But the fact that most reputable sites will refuse to host such speech—relegating it instead to low-reach blogs and other obscure properties—already acts as a natural check against its influence. And again, guaranteeing all users the basic right to self-host even the silliest crackpot conspiracy theories provides the opportunity for those rare conspiracy theories that turn out to be true to eventually reach mainstream status and inform a voting electorate.

Non-Discrimination. Non-discrimination theory, both economic and deontological, support viewpoint access rules. The economic case is the less straightforward of the two, since, as noted above, providers that take down controversial content do so for ideological reasons rather than to hamstring competitors. But economic concepts can still help to frame the nature of the exclusion when it comes to viewpoint foreclosure.

If a core intermediary refuses to provide a critical internet resource, it is useful to analyze the entry barriers that would prevent a deplatformed speaker from entering—that is, vertically integrating into—the market to obtain substitute resources.

With respect to connectivity and nameability, entry barriers are high but not insurmountable. Returning to our controversial heroine, Jane could theoretically become her own ISP, although the costs of laying down fiber to connect to the nearest internet exchange point might be exorbitant. She could also become her own registrar or potentially even her own registry operator (e.g., launching radical.jane), although ICANN could veto either effort.

But when it comes to addressability, entry barriers cannot be overcome.

By virtue of ICANN's complete control over internet naming and numbering, only five RIRs manage the world's limited IP address space, and no vacancies have ever been advertised. While Jane could theoretically create a competing network protocol and associated address space, economic network effects would doom any such effort. As Milton Mueller puts it, the Internet Protocol is the "lingua franca" of the internet, the only protocol in the internet stack for which there is no substitute.[335] Accordingly, for Jane to reach interested users, not only would each such user need to adopt Jane's competing protocol, but every network operator between Jane and her users would need to do likewise. If countless governments, tech companies, and enterprise internet users have thus far failed to upgrade the internet to the decades-old IPv6 protocol, which everyone agrees is crucial to the future of the internet, Jane's new protocol-for-misfits would have little hope. Moreover, establishing a new network protocol would not usher a new entity into the RIR market; it would create an entirely separate market and a separate internet along with it. These factors erect similarly insurmountable entry barriers when it comes to market substitutes for the routability and accessibility rights, which would require Jane to create her own global internet backbone and provide access networks for all users who wish to consume her content.

Moreover, although each of the historical rationales for common carriage has its flaws,[336] Viewpoint Access theory finds support in each. Whatever the boundaries of the universe of businesses affected with the public interest, there can be little doubt that core intermediaries fall within them (public interest rationale). The world depends on the likes of Verisign to make .com and .net domain names operational, ARIN to make network devices identifiable, and network operators to route and carry traffic from sender to recipient. Core intermediaries may or may not possess traditional market power, but high or insurmountable entry barriers protect them from any viable competition from deplatformed users (market power rationale). And governments have historically allowed such providers to self-regulate (e.g., through ICANN) precisely because they have held themselves out to the public as impartial intermediaries (holding out rationale)—at least until recently. Preventing core intermediaries from discriminating against lawful content would therefore seem to be justified under any mainstream theory of common carriage.

But how would Viewpoint Access theory address Yoo's contention that common carriage works well only for commodities with simple interfaces

335. MUELLER, *supra* note 320, at 25.

336. *See supra* section I.C.2.

and stable demand? For example, negotiations to obtain commercial internet connectivity or colo space may be highly complex, with rates and terms that depend on many factors, such as credit risk or potential for future business. If a provider charges Jane significantly higher rates than other website operators, who's to say whether such rates reflect legitimate business considerations or ideological discrimination?

Yet Viewpoint Access theory is not incompatible with highly dynamic markets. Because Viewpoint Access theory owes as much to the deontological basis of non-discrimination law as it does to the economic, viewpoint access rules could employ the same but-for rules that underlie Title VII and other deontologically-based non-discrimination regimes. For decades, those but-for rules have successfully abstracted away the subjectivity of non-commoditized markets and complex negotiations by simply asking whether an entity based its decision on an impermissible characteristic of the aggrieved party.[337] For example, the labor market is anything but commoditized. Deciding to hire one candidate over another may turn on highly subjective assessments ranging from academic pedigree to relevant experience to mere likeability. But Title VII doesn't need to dictate how employers must weigh each consideration to prevent racial discrimination. It only needs to ask whether the candidate's race affected the decision.

In the same manner, the law could ensure basic viewpoint access without extensively regulating the market for core internet services. It could do so by simply granting aggrieved website operators a private cause of action against core intermediaries for viewpoint discrimination (and the right to recover damages) where it can be proved that a core intermediary's adverse actions—whether terminating services, refusing to deal, or simply charging higher prices—were motivated by hostility to the website operator's viewpoint.

User Property Rights. Finally, Viewpoint Access theory helps to address the power imbalance between users and providers by granting users something approximating basic property rights.

At a minimum, those property rights include stable ownership or possession of IP addresses, network numbers, and domain names—the resources that most resemble traditional intangible property. But whereas all forms of intangible property represent chattels, it could be argued that the rights of addressability and nameability go further by establishing something more akin to *real* property (virtual though it may be). They provide controversial website operators with that most basic concession

337. *See* Bostock v. Clayton Cnty., __ U.S. __, 140 S. Ct. 1731, 1739–43 (2020) (explaining how Title VII claims are evaluated under a but-for causation standard).

given to all social outcasts: the right to congregate and subsist on their own land, free from the molestations of a disapproving public.

Extending this metaphor further, the rights of connectivity, routability, and accessibility could be said to operate like easements or, better yet, public roads that allow users to freely move between virtual lots.[338] Thus, Viewpoint Access theory arguably disrupts the complete privatization of cyberspace in the hands of providers by granting users their own share of that private property and reserving a modest portion of that property for public use.

2. Viewpoint Access Theory and Provider-Centric Principles

Although Viewpoint Access theory calls for intervening in private content moderation decisions, thereby shifting certain power from providers to users, it does so in ways that remain consistent with the most important principles from the provider-centric theories canvased in Part I—namely, Free Market, Provider Property Rights, Good Samaritanism, and Editorial Rights.

Free Market. While any form of interventionism, by definition, detracts from a free market ethic, one advantage Viewpoint Access theory possesses over other interventionist theories is its modesty. Far from ushering in a whole new approach to content moderation, the five internet rights merely codify the implicit social contract that has governed the internet since at least the mid-1990s.[339] Viewpoint access rules target a narrow class of core intermediaries with simple non-discrimination mandates, leaving the free market otherwise intact for the rest of the internet.

Because of this modesty, the vast majority of internet users would see no change to their online experience. Contrast this continuity with the effects that would result from applying other interventionist theories. For example, by forcing social media companies to host all lawful content, no matter how toxic, platform neutrality could significantly degrade the experience of most users. As Eric Goldman and Jess Miers have noted, forced carriage rules aimed at providers within the application layer would flood many online environments with material that most users don't want, from Nazi propaganda to conspiracy theories to potentially even

338. *Cf.* Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125, 155–57 (2005) (analogizing the internet backbone to "public roads"); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 477 (2003) ("The Internet is conceived in familiar terms, just like the public roads that lead to private properties . . . .").

339. *See supra* section II.B.

pornography.[340] By contrast, while viewpoint access rules might enable certain offensive sites to remain online that otherwise would not survive certain deplatforming efforts, users could continue to steer clear of unsavory content by simply avoiding such sites.

Moreover, Viewpoint Access theory presents a good opportunity for the left and the right to strike a deal on net neutrality. By compromising on new regulation that embodies the five internet rights, progressives could obtain the competitive non-discrimination rules they have long sought in exchange for granting conservatives the modest ideological protections they desire. In other words, by marrying the economic and deontological foundations of non-discrimination theory through narrow regulations that target only deep-stack providers, both sides could get much of what they want while avoiding the hot culture wars that rage within the application layer.

Provider Property Rights. Because the five internet rights function as forced carriage rules, they obviously interfere with the right of core intermediaries to use their hardware and software as they please. But when it comes to ensuring basic viewpoint access, that interference with provider property rights proves to be quite minor.

In the case of the addressability and nameability rights, viewpoint access rules require no carriage to speak of. As described in Part II, neither RIRs nor DNS intermediaries transmit web content as part of the core internet services they render. RIRs simply allocate IP addresses and network numbers to entities and then leave it to network operators to route internet traffic among themselves using those identifiers. DNS providers likewise grant domain names to website operators, and certain providers must provide ongoing resolution services to translate those domain names into IP addresses. But once those translation services have been performed, website operators and users are on their own to send and receive any actual content.

The accessibility and routability rights do entail carriage, since last-mile ISPs must obviously carry website content to their subscribers, and backbone operators must relay content between other networks along the transmission path. But both of these rights are better conceptualized as prohibitions against *blocking*. Under the accessibility right, ISPs must simply honor their subscribers' choices to access the websites they like rather than blocking content from websites the *ISPs* dislike. And under the routability right, backbone operators must honor IP address and network announcements between origin and destination networks rather than manipulating routing tables to make network paths appear

340. *See* Goldman & Miers, *supra* note 229, at 208–14.

unavailable for unpopular websites.

Only the connectivity right entails forced carriage in the classic sense by requiring ISPs to do business with and carry the content of customers they would otherwise avoid. However, given the long history of regulating transit operators as common carriers and the fact that ISPs could charge controversial website operators for connectivity just the same as for other subscribers, viewpoint access rules would impose trivial burdens on ISP property rights.[341]

Good Samaritanism. Viewpoint Access theory is also compatible with Good Samaritanism, rightly understood.

By "rightly understood," I mean that Good Samaritanism comes in two forms. In its basic form, the theory endows website operators with godlike power to dictate what constitutes acceptable content and to remove other content without fear of liability.[342] But that power stops at the edges of their own websites. By contrast, expansive Good Samaritanism is essentially synonymous with deplatforming or no-platforming. It operates not merely by permitting individual website operators to create safe spaces that users with discriminating tastes can choose to visit but by cleaning up the *internet itself*, ensuring that *no* unclean spaces exist, even unclean spaces that some users might want to visit.

Viewpoint Access theory is certainly compatible with basic Good Samaritanism. Consistent with its modesty, the theory would still permit each website operator to moderate as he sees fit. Enacting viewpoint access rules, therefore, would not sully any portion of the internet that a user cares to experience because that user can choose which sites to visit and which to avoid. It continues to empower Good Samaritans throughout cyberspace to create safe environments for children, marginalized groups, or those who simply prefer polite company.

But Viewpoint Access theory is not compatible with expansive Good Samaritanism because it would deny immunity to core intermediaries that leverage their deep-stack power to boot controversial content from the internet entirely.

Does that mean viewpoint access legislation would need to amend Section 230? Maybe. Section 230 applies to providers of "interactive computer service[s]," which include services and systems that "provide[] or enable[] computer access . . . to a computer server, including . . . access to the Internet."[343] This definition, taken literally,

---

341. *See* Lemley, *supra* note 82, at 537–42 (expressing openness to conceptualizing cyberspace as a place while noting that, as with real property, cyber-property rights can be subject to limitations, such as easements, that provide public benefits).

342. *See supra* section I.B.3.

343. 47 U.S.C. § 230(f)(2).

would potentially encompass network operators and perhaps even DNS providers, although it would be hard to characterize such systems as "interactive" in the conventional sense of the word. And expansive Good Samaritanism is not supported by the legislative history of Section 230. The underlying premise of Section 230 was that by immunizing content moderation, website operators could compete for different types of users by offering different flavors of acceptable use, thus fostering a diverse marketplace of content policies. Deep-deplatforming by core intermediaries, however, can destroy that diversity by imposing uniform acceptable use policies over the entire internet.

Thus, it seems unlikely that Section 230 would contradict basic viewpoint access rules. Moreover, if the definition of "interactive computer service" were so broad as to capture even core intermediaries like ISPs, then even the 2015 net neutrality rules would have been invalid under Section 230, a position explicitly rejected by the FCC.[344]

Editorial Rights. Finally, viewpoint access rules are consistent with the principles underlying the Editorial Rights theory. Even if Volokh is wrong that the content moderation practices of social media companies and other application providers don't amount to protected speech, it would be very difficult to argue that the First Amendment applies to the operations of core infrastructure providers.

Consider RIRs, which merely allocate IP addresses and do not host any third-party content. RIRs are not in the business of cultivating any kind of user experience or arranging IP-accessible websites into anything resembling a coherent speech product. RIRs are instead technical enablers of internet communications, only a step or two up from providing electricity. DNS providers likewise do not host, cultivate, or compile content. Their acts, therefore, are too far removed from expression for them to legitimately claim editorial rights in their services.

The case for editorial rights for ISPs and backbone operators fares no better. None of these core intermediaries selects content to carry, display, or promote. Each is instead hired to act as a dumb conduit for whatever data its customers elect to send or receive. Even if Nazi or Communist propaganda happens to flow through copper wires maintained by Charter or wireless spectrum allocated to AT&T, users do not associate that content with either network operator, and each operator remains free to distance itself from any such content by making statements on its own website.

Accordingly, however the battle for editorial rights shakes out when

344. *See* 2015 Open Internet Order, *supra* note 198, ¶ 386 (rejecting the argument that broadband Internet access service constitutes an "interactive computer service").

social media laws like those of Florida or Texas eventually reach the Supreme Court, it seems unlikely that any resulting editorial rights doctrine would shield infrastructure providers from regulation like basic viewpoint access rules.

IV. OBJECTIONS

In this last Part, I address what I anticipate will be the most common objections to Viewpoint Access theory and the five internet rights it entails.

A. Too Much: Internet Exceptionalism

Some might argue that guaranteeing users the right to express themselves on the internet isn't necessary because offline alternatives always exist.

Booted speakers remain free to speak in traditional public fora, such as parks, streets, and libraries; to create and distribute books, newspapers, and DVDs; and even to leverage other mass communication technologies, such as television and radio. After all, Jane's unpopular views found their first expression in a book she found that managed to survive for centuries in libraries and on bookstore shelves. Despite being kicked off the internet, Jane could still reproduce that book and pass it around to interested readers. And she could still hold rallies in the park or grant interviews to interested radio or television talk show hosts. The internet represents just one new(ish) medium in a long line of communication technologies to emerge over the last two hundred years. If the law should intervene to ensure that anyone can speak on the internet, why not require the same for radio, television, or book publishing? What makes the internet different?

Internet exceptionalism is indeed a key premise underlying Viewpoint Access theory. Implicit arguments for internet exceptionalism have been scattered throughout this Article, so I'll add only a few more explicit arguments here.

The internet differs from other forms of media in at least three ways relevant to viewpoint foreclosure.

First, other forms of mass media are generally not participatory. A movie, TV show, or radio broadcast can reach audiences in the millions, but few people have the financial resources or access to the infrastructure required to distribute content via these offline channels. As a result, these legacy media have largely remained in the hands of a professional class of content providers and cannot be used by any and every citizen or group to broadcast their views to the world. Indeed, the internet revolutionized

the media landscape precisely because it democratized both the production and the distribution of content.[345]

Second, unlike the internet, other media lack a clear dividing line between participation and exclusion. For example, Jane may fail to find a respectable publishing house, magazine, or newspaper to publish her manifesto. But at no point is she ever truly "shut out" of the world of print. She can bind and distribute her own books or perhaps even persuade a smaller, less reputable publisher to amplify her viewpoints. By contrast, unless she enjoys a basic right to viewpoint access, a website containing her viewpoints may indeed be removed from the internet altogether. The terms "online" and "offline" have meaning only because a clear line separates these two states. No such dividing line gives the terms "on-book" or "off-book" any intelligible meaning.

Third, unlike the internet, traditional media lack centralized choke points controlled by a small number of private actors who are not bound by the First Amendment. DirecTV may choose not to carry controversial channels like One America News Network,[346] but no private entity or group of private entities has the power to prevent *every* cable or satellite TV provider from doing so or to prevent every station in the country from airing an offensive radio program. As such, traditional media does not present the same opportunity for foreclosure.

While other communication technologies might exist that also manifest clear lines between participation and exclusion or that vest private entities with unchecked power to exclude users,[347] one struggles to think of any such technology that comes close to approximating the modern public sphere. The internet, quite simply, is where the people and the content are.[348] As Jack Balkin has argued, the public sphere is not fixed in its definition or destination but is instead best understood as "the space in which people express opinions and exchange views that judge what is going on in society."[349] It is for this reason that internet access, a concept that encompasses online expression, is increasingly being recognized as a human right in other countries.[350]

---

345. *See generally* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995).

346. *See* Gerry Smith, *DirecTV to Drop One America News in Blow to Conservative Channel*, BNN BLOOMBERG (Jan. 14, 2022), https://www.bnnbloomberg.ca/directv-to-drop-one-america-news-in-blow-to-conservative-channel-1.1707990 [https://perma.cc/FPH7-BNPZ].

347. For example, Meta alone controls its "metaverse."

348. Danielle Keats Citron, *How to Fix Section 230*, B.U. L. REV. (forthcoming 2023) (manuscript at 8) (on file with author) ("[T]he internet is embedded in everything we do and everywhere we go.").

349. Balkin, *supra* note 149, at 72.

350. *See Access to Internet Is a Basic Right, Says Kerala High Court*, HINDU (Sept. 20, 2019, 12:30 PM), https://www.thehindu.com/sci-tech/technology/internet/access-to-internet-is-a-basic-right-

B. Too Little: Functional Foreclosure

Others might argue that the five internet rights don't go far enough to protect users. Indeed, as I have articulated it thus far, Viewpoint Access theory provides only a floor for interventionism: the law should intervene where necessary to prevent viewpoint foreclosure, the most extreme form of exclusion. And it may do so by granting users certain *minimum* rights—the five internet rights—each of which pertains to the core infrastructure layer of the internet.

But does Viewpoint Access theory also establish a ceiling for interventionism? Should the law intervene *only* when content moderation reaches the core infrastructure layer, or does the theory allow for interventions in any higher layers of the internet stack?

Answering that question turns, in part, on whether we use actual foreclosure versus functional foreclosure as the trigger for intervening. Actual foreclosure means that a user *cannot* publish her viewpoints on the internet (in the form of a publicly accessible website) no matter her financial resources because no amount of money can give her control over the core resources she needs. Functional foreclosure means that even if a user can access the core resources that define the five internet rights, her website may nonetheless falter if she cannot access certain non-core resources that modern websites depend on and for which she cannot *practically* create substitutes.

For example, websites require security. At a minimum, to protect the identities and activities of their users, websites rely on public key encryption, which itself depends on security certificates (e.g., SSL certs) issued by private certificate authorities. If certificate authorities refuse to grant SSL certs for an unpopular website,[351] that website may be effectively prevented from offering HTTPS encryption, making it too

---

says-kerala-high-court/article29462339.ece [https://perma.cc/CN88-DRFS] (India); Andres Guadamuz, *Costa Rican Court Declares the Internet as a Fundamental Right*, TECHNOLLAMA (Oct. 2, 2010), https://www.technollama.co.uk/costa-rican-court-declares-the-internet-as-a-fundamental-right [https://perma.cc/22QU-5Y2C] (Costa Rica); Charles Bremner, *Top French Court Rips Heart Out of Sarkozy Internet Law*, SUNDAY TIMES (June 11, 2009, 2:44 PM), https://www.thetimes.co.uk/article/top-french-court-rips-heart-out-of-sarkozy-internet-law-xq8nqq0hxsv (last visited Apr. 12, 2023) (France); 1975 SYNTAGMA [SYN.] [CONSTITUTION] 5A(2) (Greece) ("All persons have the right to participate in the Information Society."); *cf.* James Vincent, *UN Condemns Internet Access Disruption as a Human Rights Violation*, VERGE (July 4, 2016, 1:33 AM), https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access [https://perma.cc/2SA5-FQJ7] (non-binding EU resolution).

351. *See, e.g.*, DIGICERT, ONLINE SERVICES ACCEPTABLE USE POLICY § A (2019), https://www.digicert.com/wp-content/uploads/2020/09/DigiCert_online-services-acceptable-use-policy.pdf [https://perma.cc/GQ3E-CDKF] (prohibiting customers from using DigiCert's security certificates in connection with "offensive" or "objectionable" activities).

risky for many users to visit.

Just as important, website operators may need to defend themselves from distributed denial-of-service (DDoS) and other volumetric attacks. Such attacks may come not only from traditional bad actors who seek to extort lucrative operators but increasingly from "hacktivists" who target objectionable websites for ideological reasons.[352] To protect themselves, many websites rely on security vendors, such as Cloudflare, which can diffuse DDoS traffic across global networks of "edge" servers to absorb volumetric attacks, passing only legitimate traffic onto web servers.[353] Yet those same viewpoints that make controversial websites the target of hacker groups can cause security vendors to want nothing to do with them. For example, in 2017, after public attention turned to toxic content on the Daily Stormer, Cloudflare terminated DDoS protection services for the site, leaving it vulnerable to attacks from "vigilante hackers" that ultimately took it down.[354]

Websites also rely on content delivery networks (CDNs) to make websites more geographically accessible by caching content in edge sites, such as colo facilities, around the world to be closer to users. Yet CDNs, like cloud computing providers, may deny service to unpopular websites, leaving them with high latencies that threaten to permanently sideline them from mainstream user engagement.

Finally, websites, like all ventures, depend on financial resources to operate and scale. Yet, as deplatforming has expanded to encompass demonetization, financial intermediaries are increasingly cutting ties with unpopular websites, drying up critical sources of external funding.[355] Even cryptocurrencies, such as Bitcoin, may be losing their utility as "free

352. *See, e.g.*, Marilyn Elias, *Anonymous Hacking Collective Declares 'Operation Blitzkrieg' Against Neo-Nazi Websites*, S. POVERTY L. CTR. (May 25, 2012), https://www.splcenter.org/fighting-hate/intelligence-report/2012/anonymous-hacking-collective-declares-operation-blitzkrieg-against-neo-nazi-websites [https://perma.cc/54JJ-6QG2] (describing efforts by the Anonymous hacking collective to take down neo-Nazi websites).

353. *See* Omer Yoachimik, *A Deep-Dive into Cloudflare's Autonomous Edge DDoS Protection*, CLOUDFLARE: CLOUDFLARE BLOG (Mar. 18, 2021), https://blog.cloudflare.com/deep-dive-cloudflare-autonomous-edge-ddos-protection/ [https://perma.cc/DM5K-92SJ] (describing Cloudflare's approach to mitigating DDoS attacks).

354. *See* Matthew Prince, *Why We Terminated Daily Stormer*, CLOUDFLARE: CLOUDFLARE BLOG (Aug. 16, 2017), https://blog.cloudflare.com/why-we-terminated-daily-stormer/ [https://perma.cc/B8X9-4L3C]; Steven Johnson, *Why Cloudflare Let an Extremist Stronghold Burn*, WIRED (Jan. 16, 2018, 6:00 AM), https://www.wired.com/story/free-speech-issue-cloudflare/ [https://perma.cc/7VAB-DVGX].

355. *See* Jack McLaughlin, *The Hidden Specter of Financial Censorship*, FORDHAM J. CORP. & FIN. L. (Nov. 20, 2021), https://news.law.fordham.edu/jcfl/2021/11/20/the-hidden-specter-of-financial-censorship/ [https://perma.cc/B5TA-UA25].

speech money" [356] as the ecosystem becomes more institutionalized and financial intermediaries begin to exercise control over who can take real money out of the system.[357]

The net result is that even if an operator can technically maintain a website on the public internet by virtue of the five internet rights, the website may nonetheless be kept effectively offline—and the viewpoints expressed on it functionally foreclosed—if security, CDN, and payment vendors all refuse to play ball. As Matthew Prince, Cloudflare's CEO, candidly acknowledged after yanking security services from Daily Stormer, "[l]iterally, I woke up in a bad mood and decided someone shouldn't be allowed on the internet."[358] If the goal is to prevent anyone from being effectively kicked off the internet, what should be done about this kind of functional foreclosure?

One option is to adopt a more expansive version of Viewpoint Access theory that would have the law intervene where necessary to prevent functional foreclosure as well as actual foreclosure.

In particular, when considering whether to intervene if a provider denies a particular internet resource, policymakers could ask two questions:

(1) Is the resource effectively necessary to operate a stable, publicly accessible website?

(2) Could an internet user, with reasonable financial means, create a substitute resource?

If the answer to the first question is yes, but the answer to the second question is no, then the law might intervene to prevent that provider from discriminating against lawful users based on ideology. Applying these criteria would likely bring some resources from the infrastructure layer into scope (though probably not from the application layer). For example, under these criteria, we might consider additional rights of security and monetization (because it would likely cost millions of dollars to build edge sites around the world or to build a substitute payment network) but perhaps not an additional right of cacheability (because a website can still operate even if it is slow).

These questions sound in economic theory—in particular, market entry

---

356. *See* Peter McCormack, *Gab's Andrew Torba on Why Bitcoin Is Free Speech Money*, MEDIUM (Feb. 10, 2019), https://medium.com/hackernoon/gabs-andrew-torba-on-why-bitcoin-is-free-speech-money-dcbe15be5e43 [https://perma.cc/RR7J-L32Y].

357. *See* Erin Carson, *Gab Says It Was Kicked Off Coinbase*, CNET (Jan. 7, 2019, 12:16 PM), https://www.cnet.com/culture/gab-says-it-was-kicked-off-coinbase-again/ [https://perma.cc/WLS5-HYG6].

358. Johnson, *supra* note 354.

barriers or essential facilities.[359] However, because a foreclosed user seeks these resources not to compete with established players but only to use them as a consumer, it remains to be seen how competition doctrine could inform our approach to functional foreclosure. Thus, I leave it to a future project (or others) to consider whether economics, deontological ethics, or other disciplines could be brought to bear in determining whether to adopt a more expansive version of Viewpoint Access theory. I also leave it to another day to consider whether the above criteria should provide a ceiling for interventionism—that is, to say that the law should *not* intervene unless actual or functional foreclosure occurs—or whether Viewpoint Access theory can be supplemented and complemented by other interventionist theories, such as those that pertain to the application layer.

C. Too Messy: Unclean Hands

Even if Viewpoint Access theory falls within the goldilocks zone between too much intervention and not enough, some might argue that we shouldn't construct a theory of interventionism in response to certain new forms of deep deplatforming because most examples of deep deplatforming aren't clean. That is, it can be hard to find examples of deep deplatforming or viewpoint foreclosure where the intermediary terminated services *solely* because it opposed a user's viewpoint.

More commonly, core intermediaries can, and do, claim that they terminated services for other reasons, such as because a user violated viewpoint-neutral terms of service or engaged in suspicious or potentially illegal behavior. For example, Hurricane Electric, an ISP that terminated internet access service for the parody site chamber-of-commerce.us, which mocked the U.S. Chamber of Commerce's stance on climate change legislation (implicating the connectivity right), claimed to base its decision on a (dubious) copyright claim rather than on ideology.[360] GoDaddy, which claims not to censor lawful online expression, suspended the domain name ar15.com (implicating the nameability right) for hosting user content that allegedly incited violence—although providers often use the term "incitement" interchangeably with lawful speech that merely celebrates or that could potentially lead to violence in

359. *See, e.g.*, Nikolas Guggenberger, *The Essential Facilities Doctrine in the Digital Economy: Dispelling Persistent Myths*, 23 YALE J.L. & TECH. 301, 313–31 (2021) (arguing for a resurrection of the essential facilities doctrine to cabin the power of incumbent technology firms benefiting from network effects and other lock-in dynamics).

360. Ryan Singel, *Microsoft Takes Down Whistleblower Site, Read the Secret Doc Here*, WIRED (Feb. 24, 2010, 7:03 PM), https://www.wired.com/2010/02/microsoft-cryptome/ [https://perma.cc/3KJJ-9G67].

some undetermined way.[361] And LACNIC apparently revoked DDoS-Guard's IP addresses (taking Parler offline and implicating the addressability right) because it did not regard DDoS-Guard as a legitimate Belizean entity under LACNIC's terms of service.[362]

Clearly, service providers have an interest in not having their services used to facilitate tortious or illegal conduct. And given the scarcity and rising cost of IPv4 addresses, RIRs have valid interests in preventing fraud and ensuring that address space remains available in underserved regions.

But unlike higher-stack providers, core intermediaries have at most an attenuated connection to illegal activity that utilizes their services and resources. That illegal internet activities depend on IP addresses for communication differs little from the fact that drug dealers reside in houses with street addresses, which enable prospective buyers to locate them. Domain names likewise might be compared to business tradenames—useful in facilitating transactions but hardly an instrumentality of crime. And in neither case does the core intermediary even carry any illegal or infringing content through its pipes. While the pipes operated by network operators may carry illegal or infringing content, the same could be said for copper wires maintained by telephone companies or roads on which trucks carrying contraband drive.

These connections are far too remote to argue that core intermediaries should play any role in policing illegal conduct. Therefore, just as telephone companies have been prohibited from terminating service based merely on their suspicion that a subscriber is engaged in illegal activities,[363] viewpoint access rules should likewise protect users from amateur law enforcement at the hands of core intermediaries.[364]

While core intermediaries may be in a better position to detect

---

361. *See, e.g.*, 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/AC5F-RFMM] (concluding that a user statement expressing the hope of seeing certain harm come to Jews constituted an "incitement of violence"); *see also* Allemann, *supra* note 11 ("[I]t seemed that GoDaddy suggested the content on the site could *lead* to violence, even if it didn't directly call for it." (emphasis added)).

362. Krebs, *supra* note 15.

363. *See, e.g.*, Andrews v. Chesapeake & Potomac Tel. Co., 83 F. Supp. 966, 968–69 (D.D.C. 1949) ("A public utility may not deprive a member of the public of his rights to service merely because it receives a notice from a law enforcement agency that he is using the service for illegal purposes."); Nadel v. N.Y. Tel. Co., 170 N.Y.S.2d 95, 96–98 (N.Y. Sup. Ct. 1957) (prohibiting a telephone company from removing telephone service to a customer with eleven previous arrests based on the mere assumption that the customer would likely use the service for illegal purposes).

364. Note that Section 230 immunizes higher-stack providers, which are much closer to being instrumentalities of crime, from liability for illegal acts of their users. *See* 47 U.S.C. § 230(e) (preempting state laws, including state criminal laws, that would hold online service providers liable for illegal content posted by users).

violations of *their own* policies, intermediaries could still apply even viewpoint-neutral terms of service in a biased manner. For example, DDoS-Guard saw its address space revoked because it used a shell company to register with LACNIC, even though foreign corporations often create local subsidiaries (with no employees or assets) to obtain licenses granted only to local entities. Or, if LACNIC acted as it did because DDoS-Guard did not primarily serve users in South America, LACNIC no doubt knew that such requirements are widely ignored and rarely enforced. Terminations based on a core intermediary's terms of service, thus, present ample opportunities for selective enforcement or questionable interpretation in service to ideological ends.[365]

Given these risks, what can be done to prevent core intermediaries from using their terms of service as a backdoor for viewpoint foreclosure?

I think we can reject outright any suggestion to regulate how core intermediaries craft and enforce their terms of service. Since Viewpoint Access theory does not rest primarily on economic principles of non-discrimination, core intermediaries should not be regulated as utilities.

Instead, consistent with the deontological basis for our theory, viewpoint access rules could borrow from Title VII and its analogs. Based on its broad prohibitions against race-based employment discrimination, courts have interpreted Title VII to prohibit employers from terminating Black employees, even for violating race-neutral workplace rules, if the employers have otherwise failed to discipline white employees for the same violations.[366] Similarly, victims of viewpoint foreclosure could bring claims against core intermediaries who terminate them for violating the latter's term of service, and prevail, if it could be shown that ideological hostility played a key role in how an intermediary interpreted or enforced its house rules.[367]

Finally, as a pragmatic matter, I should note that not all instances of deep deplatforming or viewpoint foreclosure arise because a provider

---

365. A provider that wishes to target an unpopular group need find only a single alleged violation to revoke services, no matter how minor the infraction compared to the group's overall activity. *See* Betsy McCaughey, *GoFundMe's $10M Shutdown of Canadian Truckers Shows It's Time to Rein in Big Tech*, N.Y. POST (Feb. 7, 2022, 7:20 PM), https://nypost.com/2022/02/07/gofundmes-10m-shutdown-of-canadian-truckers-shows-its-time-to-rein-in-big-tech/ [https://perma.cc/7JKT-ABFB] (noting that GoFundMe demonetized the Canadian truck protesters based on only three instances of minor illegality while continuing to fund protests in Portland that "set fire to police stations, vandalized city hall, wielded weapons and injured police officers").

366. *See* EEOC v. Kohler Co., 335 F.3d 766, 775–77 (8th Cir. 2003).

367. Although viewpoint access rules borrow from Title VII, I do not take a position at this time on how central ideological hostility must be to a provider's decision for a plaintiff-user to recover. *Compare* Bostock v. Clayton Cnty., __ U.S. __, 140 S. Ct. 1731 (2020) (motivating factor), *with* Comcast Corp. v. Nat'l Ass'n of Afr. Am.-Owned Media, __ U.S. __, 140 S. Ct. 1009 (2020) (but-for causation).

wishes to get involved. Perhaps just as common are situations in which a provider would prefer to steer clear of culture wars, but public pressure mounts for it to act.[368] To be sure, core intermediaries are less vulnerable to public pressure because they have fewer competitors, and members of the public often do not directly patronize certain lower-layer providers, such as DNS intermediaries and RIRs. But deplatforming campaigns have proven very effective at persuading registrars, and the Parler saga shows that even RIRs may feel compelled to step in.

As a result, some core intermediaries have bemoaned their fate in having to either violate implicit internet neutrality principles or else risk coordinated boycotts, and some have even called for neutrality laws to protect *them* from this predicament. After effectively booting Daily Stormer from the internet by terminating security services in response to public pressure, Cloudflare's CEO remarked that "[n]o one should have that power."[369] The CEO of Namecheap, a popular domain registrar, likewise agonized over his decision to suspend domain names associated with extremist websites and the fact that standing for free speech might bankrupt his company and cause over a thousand employees to lose their jobs.[370] He therefore called for "a set of guidelines" and a "clear judicial process" that would enable registrars to "remain neutral."[371] Thus, far from subjecting them to onerous, unwanted regulation, many core intermediaries might welcome the ability to tell the Ron Guilmettes of the world that as much as they might share his contempt for a given website, the law simply ties their hands from doing anything about it.[372]

---

368. *See* Bambauer et al., *supra* note 94, at 1053 ("[Some] 'moderation' may amount to little more than platforms bending to the demands of their most vocal users.").

369. Johnson, *supra* note 354.

370. Kirkendall, *supra* note 361.

371. *Id.*

372. Another objection some have privately offered to me is that the law need not regulate private intermediary conduct because the state could more easily prevent viewpoint foreclosure by simply offering public alternatives. While it is true that the state could theoretically operate application-layer fora that welcome all lawfully expressed viewpoints (assuming core intermediaries would be legally prohibited from pulling resources from even those fora), the state could not necessarily create or reserve alternative core resources to enable all lawful U.S. residents to operate their *own* websites. For example, the federal government has been delegated authority to manage the .us top-level domain and also holds millions of usable IP addresses. Assuming ICANN and ARIN would not stand in the way (a reasonable assumption), the federal government could make these resources available to otherwise deplatformed private websites, thus guaranteeing the addressability and nameability rights. But to ensure the remaining rights, the federal government would not only need to operate its own coast-to-coast network (ensuring the connectivity and routability rights) but other internet users would need to rely on the federal government for primary internet access (to account for the equally crucial accessibility right). Put differently, the federal government would essentially need to nationalize the entire domestic network that powers the internet. Such a massive undertaking would be far more

CONCLUSION

The story of the internet is one of continual innovation. From resilient protocols to faster transmission media to mass sharing applications like social media, the relentless drive for optimization (and riches) has caused the internet to advance at an exponential rate. This same drive for optimization has been no less present when it comes to content moderation, where those opposed to bigotry and disinformation have not been content to fall back on traditional methods of cleaning up the internet just because that's the way we've always done things. Instead, those who desire a healthier, more tolerant internet have, quite understandably, looked for ever cleverer and more efficient ways to fight extremism.

But few things in this world are unalloyed goods. If we've learned anything from the last ten years, it's that more is not always better. Applications can in fact make it *too easy* to speak one's mind to the world, thereby lowering the transaction costs of trolling, bullying, and whipping up mobs. And free services are not unambiguously better than comparable paid services, especially if the former are built on business models that profit from outrage and polarization.

If the developments of the last ten years have engendered a healthy skepticism of technological advances, then innovations in content moderation should be no less immune from scrutiny. While infrastructural neutrality was the product of convention rather than law, it makes eminent sense why core intermediaries should stay out of the content moderation game and why, if those conventions are now breaking down, the law should step in to shore them up. Viewpoint foreclosure does not merely represent the next logical step in the evolution of content moderation; it represents the logical *end* of an unbounded campaign against unpopular viewpoints and individuals. And it represents the point at which culture and ideology supplant stability and sound engineering as the guiding principles of internet governance.

This Article is not the first to question the unrelenting march to shut down offensive online speech by moving down the internet stack, but it is the first to identify viewpoint foreclosure as a clear line of demarcation between acceptable and unacceptable deplatforming practices and to offer a new theory of interventionism premised on basic viewpoint access. Not only does Viewpoint Access theory strike the right balance between user and provider rights, embodying the best principles of other interventionist theories while discarding their flaws, but it has the advantage of clear, administrable rules—the five internet rights—that naturally emerge based

---

disruptive than simply enacting legislation to prevent a small group of core intermediaries from engaging in discriminatory practices.

on the architecture of the internet.

Whether I have perfectly articulated the fundamental rights needed to instantiate Viewpoint Access theory could certainly be debated. Perhaps a broader conception of viewpoint access—one that includes additional rights, such as security, cacheability, or monetization—is needed to prevent functional foreclosure. Or perhaps regulatory mechanisms other than private suits could be used to enforce the five internet rights more effectively.

But if we at least start with the modest premise that all groups and individuals should have the basic right to lawfully express themselves on the internet in a stable, authoritative, and publicly accessible manner, then reasonable minds could disagree about precisely which rights should flow from that premise, whether now or in the future as the internet evolves. It is therefore my hope that others may build, improve, and even *innovate* upon Viewpoint Access theory to craft sound internet policies as we strive to thoughtfully balance competing rights in the never-ending challenge that is content moderation.