The Decentralized Web and the Future of Section 230

Author:

Andrea O'Sullivan[a]

November 2022

Working Paper

The Center for Growth and Opportunity at Utah State University is a university-based academic research center that explores the scientific foundations of the interaction between individuals, business, and government.

This working paper represents scientific research that is intended for submission to an academic journal. The views expressed in this paper are those of the author(s) and do not necessarily reflect the views of the Center for Growth and Opportunity at Utah State University or the views of Utah State University.

[a] Andrea O'Sullivan is the former Director of the Center for Technology and Innovation at the James Madison Institute.

The Center for
Growth and Opportunity
at Utah State University

Introduction

Section 230 of the Communications Decency Act of 1996 significantly influenced the present-day internet.[1] By clarifying that "interactive computer services" would not be held liable for either the content provided by others or restrictions on access to objectionable material,[2] Section 230 created a space wherein platforms could build the viable businesses that have come to dominate the internet experience.

With this success came controversy. Critics of content moderation decisions came to view Section 230 liability protections as a de facto subsidy for censorious platforms to limit public speech[3] or to be less than judicious in limiting speech.[4] Free speech advocates have worked to pare back Section 230[5] or tie liability protections to defined platform obligations intended to promote a healthier range of discussion.[6] However, as Section 230 advocates point out, the text of the law explicitly encourages "action(s) voluntarily 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, whether or not such material is constitutionally protected."[7]

Section 230 has become something of a red herring in the debate over free speech and platform policies.[8] Much of the conversations devolve into relitigating the legislative record[9] on Section 230—what the text did or did not say or imply. In the meantime, the issue of whether users and the body politic are well served by dominant content moderation standards remains open.

The limitations of market mechanisms to address these concerns were highlighted in the industrial deplatforming of alternative applications such as Parler[10] as well as the political establishment's hostility towards the idea of Twitter being purchased and run by new free speech–friendly management.[11]

Perhaps these liability protections encouraged the internet industry to foster centralized platforms that could make such content decisions. By lowering the cost of content moderation, liability protections might have artificially induced a technological form that would otherwise be

[1] 47 U.S.C. §230.

[2] Section 230 is not a blanket liability shield, and there are legislative carveouts that address targeted issues such as intellectual property, child protection, and certain personal health and financial data.

[3] "Senator Hawley Introduces Legislation to Amend Section 230 Immunity for Big Tech Companies," Senator Josh Hawley, June 19, 2019, https://www.hawley.senate.gov/senator-hawley-introduces-legislation-amend-section-230-immunity-big-tech-companies.

[4] Elizabeth M. Jaffe, "Imposing a Duty in an Online World: Holding the Web Host Liable for Cyberbullying," *Hastings Communications and Entertainment Law Journal* 35, no. 2 (2013): 277, https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol35/iss2/2/.

[5] "Senator Hawley Introduces Legislation."

[6] "Blackburn & Colleagues' EARN IT Act Closer to Becoming Law," US Senator Marsha Blackburn of Tennessee, February 15, 2022, https://www.blackburn.senate.gov/2022/2/blackburn-colleagues-earn-it-act-closer-to-becoming-law.

[7] 47 U.S.C. §230.

[8] Reese Bastian, "Content Moderation Issues Online: Section 230 Is Not to Blame," *Texas A&M Journal of Property Law* 8, no. 2 (2022): 43–72, https://doi.org/10.37419/JPL.V8.I2.1.

[9] Robert Cannon, "The Legislative History of Senator Exon 's Communications Decency Act: Regulating Barbarians on the Information Superhighway," *Federal Communications Law Journal* 49, no. 1 (1996): 51, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1115&context=fclj.

[10] Andrea O'Sullivan, "Route Around Deplatforming with Decentralized Tech," *The American Conservative*, March 11, 2021, https://www.theamericanconservative.com/articles/route-around-deplatforming-with-decentralized-tech/.

[11] J. Robert McClure III, "Elon Musk Faces Uphill Battle to Make Twitter More Free," *Washington Examiner*, May 3, 2022, https://www.washingtonexaminer.com/opinion/op-eds/elon-musk-faces-uphill-battle-to-make-twitter-more-free.

uneconomical, similar to how intellectual property protections protect certain business practices. Lacking a counterfactual, these speculations are of purely intellectual interest.

The development of more decentralized platform alternatives may have been inevitable. The profitability of centralized platforms (partially made possible by Section 230 protections) has resulted in challenges for the user experience. Many technologists have been deeply dissatisfied with the poor levels of user data sovereignty and open communication afforded by dominant centralized standards. Accordingly, many projects have sought to step over these fault lines altogether by developing decentralized and open-source alternatives.[12]

This paper will place the debate over Section 230 in the context of decentralized and federated platforms—networking environments enabled by communally–agreed upon standards of computing and norms. Such technologies can empower users with more control over their platform experience while providing a more granular set of tools for individualized content curation.

I will examine two working projects that embody two approaches to the problem: the Matrix protocol and the Urbit ecosystem. In these systems, there is no one centralized entity onto which liability could be placed or removed. Much of the controversy over Section 230 becomes moot, as the user who puts forth the controversial speech is the only one with control over that content.

The Internet before and after Section 230

The birthday of the internet is traditionally understood to be January 1, 1983.[13] This is the day that the world's extant computer networks, such ARPANET and CSNET, established the Transfer Control Protocol/Internetwork Protocol (TCP/IP) standard, which allowed different networks to communicate with each other and therefore created the "network of networks" that we know and love (or perhaps loathe) today. "Online" communications had taken place within self-contained academic and military research networks since the 1960s, and "the internet" of 1983 was vastly different than the platform-dominated superstructure we now inhabit. But it's not a bad starting point.

This early internet was characterized by human-scale communities[14] of mostly technical users talking about professional and personal interests on the Usenet discussion system.[15] This unique collection of (mostly) sophisticated users tended to adjudicate whatever issues that arose. Informal norms of manners and content management emerged independently.[16] Thus, it is no surprise that questions of liability and content did not arise until the development of a broader, less human scale web.

Early internet users that had not been onboarded via professional research institutions usually gained access through academic enrollment. University students in the 90s would be given Usenet

[12] For an exhaustive list, see *Alternative Internet* (2013; repr., Recentralize.org, 2022), https://github.com/redecentralize/alternative-internet.

[13] "A Brief History of the Internet," University System of Georgia, Online Library Learning Center, accessed July 5, 2022, https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml.

[14] Jonathan L. Zittrain, "Three Eras of Digital Governance," SSRN Scholarly Paper (Rochester, NY, September 23, 2019), https://doi.org/10.2139/ssrn.3458435.

[15] Michael Hauben and Ronda Hauben, *Netizens: On the History and Impact of Usenet and the Internet* (Washington, DC, USA: IEEE Computer Society Press, 1997), https://dl.acm.org/doi/abs/10.5555/263951.

[16] Hauben and Hauben, *Netizens.*

access and a quick tutorial, giving rise to the early internet joke of the "September problem."[17] Fall registration would beget a wave of new users unaccustomed to established norms and expectations of behavior. But these internet freshmen would eventually be assimilated into Usenet culture.

This stopped being the case after the "Eternal September" when Usenet access was expanded to ISPs used by the general public as well as the AOL Usenet gateway service in 1994.[18] Now, September would never end, and new users would flood in without necessarily becoming socialized to Usenet folkways. In other words, the scale of internet communities began growing at a rate where informal norms of behavior were insufficient to adjudicate online disputes.[19] The legacy court system needed to get involved.

These internet disputes broke out amidst a long-developed body of common law surrounding damages in communications. Different liability thresholds would be triggered depending on an actor's closeness to the dissemination of content. An entity that actively edited or curated the communications, such as a newspaper or book publisher, would be more strictly liable because of its editorial role. An entity that merely allowed for the sale or distribution of already edited material, such as a newsstand or bookstore, would be subject to lower standards. Passive common carriers, such as telephone operators, would be subject to even lower liability thresholds, holding virtually no liability for passive routing.

The first challenge came with *Cubby v. CompuServe* (1991), a case involving defamatory remarks made about a business posted on one of the forums that CompuServe hosted.[20] The defendant argued that CompuServe functioned as a publisher of the materials on its forums. Therefore, because the posted materials were harmful to the business, CompuServe owed damages. The court disagreed, ruling that CompuServe had acted as a mere distributor of content, rather than a publisher, and was therefore not liable for damages caused by the user-submitted content. Rather, defendants in this kind of situation would need to instead pursue actions against the user who posted the content.

This was an attempt to harmonize the new realities of internet culture and communities with established precedent in publishing law. Analogies can be made with the historical development of the legal treatment of bookstores, newsstands, and wire services.[21] The courts had traditionally found that liability is determined by whether or not an entity was acting as a publisher actively vetting, producing, and editing content (liable), or a distributor merely selling the products offered by publishers (less-liable).

However, this approach did not stick. A similar case, *Stratton Oakmont v. Prodigy* (1995) came before the New York Supreme Court.[22] It also involved an online company, Prodigy Services, that hosted a forum where users could discuss various matters. A business sued Prodigy for damages after its founder and reputation were negatively discussed on the "Money Talk" bulletin board.

[17] Bradley Fidler, "Eternal October and the End of Cyberspace," *IEEE Annals of the History of Computing* 39, no. 1 (2017): 6–7, https://doi.org/10.1109/MAHC.2017.9.

[18] Fidler, "Eternal October."

[19] Brian S. Butler, "Membership Size, Communication Activity, and Sustainability: A Resource-Based Model of Online Social Structures," *Information Systems Research* 12, no. 4 (2001): pgs. 346–362, https://doi.org/10.1287/isre.12.4.346.9703.

[20] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

[21] Brent Skorup and Jennifer Huddleston, "The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation," *Oklahoma Law Review* 72, no. 3 (2020): pgs. 635–673, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3501713.

[22] Stratton Oakmont, Inc. v. Prodigy Services Co., 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

In this case, the court ruled that Prodigy was indeed liable for the user-submitted speech. Its reasoning was that because Prodigy had established community guidelines that moderated user-submitted content, the service was curating and editing content and constituted a publisher. Therefore, Prodigy would indeed be open to lawsuits for damages due to user-submitted content.

The inconsistencies in this developing body of precedent were quickly apparent to a forward-looking group of legislators.[23] If these decisions held, then the law could effectively encourage totally unmoderated spaces to avoid triggering liability. Good faith actors who attempted to set decency standards on their websites would be considered curators and therefore subject to harsher standards than those who did not attempt any moderation at all. Hence the "decency" bit of the Communications Decency Act. Alternatively, internet services that did choose to moderate content despite this law would be incentivized to be extremely aggressive, since they would rather err on the side of caution than be exposed to possible lawsuits for any (even remotely) inflammatory content. This is why many commentators refer to a possible "chilling effect" with the repeal of Section 230.[24]

Section 230 was added to the Communications Decency Act to address inappropriate online speech. It reads:

> *(1) Treatment of publisher or speaker*
>
> *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*
>
> *(2) Civil liability*
>
> *No provider or user of an interactive computer service shall be held liable on account of—*
>
> > *any action voluntarily 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, whether or not such material is constitutionally protected; or*
> >
> > *any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).*[25]

This provision was intended to solve the dilemma created by the developing body of internet case law where online service providers might be encouraged to be either overly censorious or totally immoderate to avoid triggering costly litigation. It clearly exempts actions taken to limit access to objectionable material (allows curation) as well as actions taken to allow access to the same (allows open fora).

[23] Ashley Johnson and Daniel Castro, "Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved," Information Technology & Innovation Foundation, February 22, 2021, https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved.

[24] David Sheridan, "Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet," 61 *Alb. L. Rev.* 1 (1997–1998): 147.

[25] 47 U.S.C. § 230.

The immediate impact of Section 230 was to halt the developing body of common law being forged through internet speech–related litigation.[26] Cases involving online speech and damages were instead routed through state and federal courts deciding how to apply Section 230.[27] Many early defamation claims against websites soliciting third-party reviews were thrown out of court due to intermediary liability.[28]

Further cases cemented the legal understanding of Section 230's range of applications. Notably, *Zeran v. America Online, Inc.* examined the question of whether an interactive computer service had a duty to remove and correct false or defamatory statements after being notified by a victim. This is known as notice-based distributor liability.[29] The court disagreed with the defendant's argument that interactive computer services still had notice-based distributor liability under Section 230, maintaining that Congress intended to prioritize building up the internet ecosystem and this kind of liability ran counter to that goal.

Today, Section 230 has become something of a household name. This law overseeing content disputes online has grown from a largely accepted and uncontroversial piece of policy to a top-line political talking point. But the laws and ideas that have been promulgated to "fix" Section 230—whether to allow more right-leaning political content or to clamp down on the same by limiting or removing liability protections—would likely exacerbate such problems more than resolve them.

Lacking Section 230 protections, computer service providers would have incentives to either remove all but the blandest content or keep everything, including the filthiest communications. This environment would also likely encourage platform largeness and concentration, as smaller endeavors would lack the infrastructure and resources to build liability-minimizing systems or acquire legal resources to fight off challenges.[30]

Technology Design and User Sovereignty

This is not to say that the issues raised by Section 230 critics are irrelevant or non-existent. They are pressing and dire. The problem is that policy may not be the best mechanism to address the question of user control online.

The design of technology is of great import for user sovereignty.[31] Centralized platforms imply centralized control of content, data, and even behavior.

Our contemporary computing experience is rooted in the fertile grounds of Bell Labs, General Electric, and MIT, all of which partnered in 1969 to develop a time-sharing OS that would

[26] Jonathan Zittrain, "A History of Online Gatekeeping," *Harvard Journal of Law and Technology* 19 (2006): 253–298, http://cyber.law.harvard.edu/publications/2006/A_History_of_Online_Gatekeeping.

[27] David S. Ardia, "Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of Intermediary Immunity Under Section 230 of the Communications Decency Act," 43 *Loyola of Los Angeles Law Review* 43, no. 2 (2010): 373–506, https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=2685&context=llr.

[28] Jeff Kosseff, "Defending Section 230: The Value of Intermediary Immunity," *Journal of Technology Law & Policy* 15, no. 2 (2010):124–158, https://scholarship.law.ufl.edu/jtlp/vol15/iss2/1.

[29] *Zeran v. America Online, Inc.*, 958 F. Supp. 1124 (E.D. Va. 1997).

[30] Ryan Nabil, "Why Repealing Section 230 Will Hurt Startups and Medium-Sized Online Businesses," Competitive Enterprise Institute, February 1, 2021, https://cei.org/blog/why-repealing-section-230-will-hurt-startups-and-medium-sized-online-businesses/.

[31] Andrea O'Sullivan, *Deplatforming and Freedom: A Primer for Policy*, James Madison Institute, March 2021, https://www.jamesmadison.org/wp-content/uploads/2021/04/PolicyBrief_Deplatforming_Mar2021_v02.pdf.

allow multiple users to access a mainframe at the same time.[32] This Multiplexed Information and Computing System (Multics) eventually gave way to the Uniplexed Information Computing Service, a backronym play on words typical of computer scientists to sound like "eunuchs," or "Unix."[33] Unix was unveiled to the public at the 1973 Association of Computing Machinery symposium.[34] It quickly became popular for its introduction of multi-user access, hierarchical file system management, asynchronous processing, portability, and built-in networking capabilities.[35]

This system was a paradigm shift in how computers could talk to each other. Developers could now easily collaborate on building computer programs. The client-server model that separates information providers (servers) and requesters (clients) married the Unix programming environment to afford a decentralized computer experience. Unix spread in popularity among academic and research communities through new versions such as Berkeley Software Distribution (BSD) and Linux, before eventually becoming a standard of commercial offerings for the broader public, such as Apple's Mac OS X.

This commercialization and the general process of onboarding the public into networked computing enables great scale. Expert computer users at well-capitalized institutions can run a server how they want, and motivated hobbyists can run their own servers for things like email and media, though the latter is fairly uncommon.

Mostly, people outsource such operations to third parties. This is part of why companies like Meta, Alphabet, Microsoft, and Apple have become so successful. It is too complicated for most people to run their own music server that their devices (clients) can access. Rather, they purchase a subscription with Apple Music or YouTube Music that streams it over the internet. We don't set up servers with our photos and videos that we can share to the world. We post them to our Facebook and Instagram pages for our friends and family to see. Most of us don't even set up our own webpages anymore (where we could rant to the world about whatever political topic we want). We have third-party hosted websites, managed through third-party publishing platforms, monetized through third-party payment services. Each of these third parties affords one more lever of control by which we can potentially be deplatformed.

Some projects aim to route around deplatforming by building tools to make it easier or clearer to run one's own server to access a service.[36] This is the model of projects like Matrix, Mastodon, and XMPP.[37] Users can opt to run their own server to host chat and media, or use a third-party server, like a friend's, or use one provided by the service itself. Servers can choose which users and other servers to connect with or blacklist. This allows some degree of private moderation and dispute resolution within the service community.

[32] David Fiedler, "The Unix Tutorial, Part 1: An Introduction to Features and Facilities," *Byte Magazine*, August 1983, pages 186–211, available at Internet Archive: https://archive.org/details/byte-magazine-1983-08/page/n187/mode/2up?view=theater.

[33] This was all in the pursuit of a better programming environment to launch video game side projects. See Dennis M. Ritchie, "Space Travel: Exploring the Solar System and the PDP-7," 1998, https://www.bell-labs.com/usr/dmr/www/spacetravel.html.

[34] Dennis Ritchie and Ken Thompson, "The UNIX Time-sharing System," *SOSP '73: Proceedings of the Fourth ACM Symposium on Operating System Principles* (January 1973): https://doi.org/10.1145/800009.808045.

[35] Richard Stallman, "New UNIX Implementation," net.unix-wizards, September 27, 1983, ironically available at: https://groups.google.com/g/net.unix-wizards/c/8twfRPM79u0/m/1xlglzrWrU0J.

[36] O'Sullivan, "Route Around Deplatforming."

[37] Jay Graber, *Ecosystem Review*, Twitter Blue Sky, January 2021, https://matrix.org/_matrix/media/r0/download/twitter.modular.im/981b258141aa0b197804127cd2f7d298757bad20.

Other projects seek to rewrite the computing environment that gave rise to mostly-corporate cloud computing. The most prominent of these is Urbit, but other examples include Pinecone[38] and CJDNS.[39]

The Matrix Protocol

The Matrix protocol is an "open standard for interoperable, decentralized, real-time communication over IP."[40] Its genesis was housed by the Israeli communications company Amdocs in 2014 as part of a "unified communications solution."[41] Amdocs employees Matthew Hodgson and Amandine Le Pape sought solutions for the problems created by having to juggle multiple chat clients. Some contacts use Facebook Messenger to communicate, others use Skype, still more use WhatsApp or Viber.[42] Then there is email, SMS, Slack, Google Chat, and Discord.[43] Managing all of the credentials and social relationships and (for the sovereignty-minded) hosting duties on top of that is a pain.

This is why Matrix was created. The project quickly won interest and awards, particularly in Europe, for its ambitions to promote interoperability among various communications options.[44] European governments have proven surprising allies in the quest to build a more federated messaging environment, with the French[45] and German[46] governments both funding the project and adopting its technologies into custom-built communications products.

The project eventually broke away from Amdocs and became a UK-based venture, New Vector Limited, which continued development of Matrix along with its client, Vector (later renamed Riot and then Element).

A good way to conceptualize the Matrix protocol is in comparison to a federated technology that most people use every day: email. There is no single email service that all of us must use to communicate with each other. Nor must we maintain separate email accounts on separate services in order to communicate with the people who signed up for each "walled garden," as we do for many chat services.

Rather, we can set up an email account with a third-party service or run our own email server and then communicate with anyone who uses the common protocols that power email: SMTP, POP, and IMAP. Likewise, with Matrix, there is no central clearinghouse for messaging that everyone must live with, nor are there walled gardens that are impenetrable by design. There is an underlying protocol that people can use to message each other no matter the hosting configuration.

[38] See "Growing Pinecones for P2P Matrix," https://fosdem.org/2022/schedule/event/matrix_p2p_pinecone/.

[39] See https://github.com/cjdelisle/cjdns.

[40] "Introduction," Matrix.org, accessed June 5, 2022, https://matrix.org/docs/guides/introduction.

[41] "Amdocs Unified Communications Solutions," archived October 3, 2014, https://web.archive.org/web/20141003202858/http://www.amdocs.com/Products/digital-lifestyle-services/Pages/unified-communications.aspx.

[42] "Active Millennial Usage Reach of the Most Popular Mobile Messaging Apps Worldwide as of 3rd Quarter 2014," Statista, February 11, 2015, https://www.statista.com/statistics/388220/mobile-messenger-app-reach-millennial/.

[43] "Bridges.jpg (Matrix.org Twitter Graphic)," https://brendan.abolivier.bzh/images/enter-the-matrix/bridges.jpg.

[44] Remi Scavenius, "Award Winners of the WebRTC 2014 Conference & Expo," Upperside Conferences Blog, archived March 15, 2015, https://web.archive.org/web/20150315032553/http://blog.uppersideconferences.com/award-winners-webrtc-2014-conference-expo/#.VZBLdbIVhBc.

[45] Matthew Hodgson, "Matrix and Riot Confirmed as the Basis for France's Secure Instant Messenger App," Matrix Blog, April 26, 2018, https://matrix.org/blog/2018/04/26/matrix-and-riot-confirmed-as-the-basis-for-frances-secure-instant-messenger-app.

[46] "The Bundeswehr Builds on Matrix," Element Blog, https://element.io/case-studies/bundeswehr.

To use Matrix, one must first set up an account on a Matrix client. The most popular is Element, created by the original developers, but third-party alternatives such as Fluffychat, Ditto Chat, and NeoChat are also available.[47] Users can opt to use the client's servers or a private configuration. IDs are tied to the server and may be linked with other credentials, such as emails and phone numbers. Users can then browse the rooms set up by other users on various servers or create their own and invite others to join. Matrix comes integrated with video and web calling.

There are also options to "bridge" into existing services such as SMS, Slack, Skype, Facebook Messenger, Discord, Google Chat and Hangouts, Telegram, WhatsApp, and Twitter.[48] In other words, Matrix users can connect these existing accounts to they are accessible within their Matrix client. This brings about the interoperability aimed for by project founders. However, bridging is often incomplete and difficult to set up. Further complications arise in terms of encryption and security.[49]

Moderation is handled primarily at the server and room level. The project states that its "goal is to provide a free and open global network for interoperable e2e-encrypted communication, without sacrificing usability, and so liberate users from being trapped in the proprietary communication silos which have become commonplace today."[50] As such, moderation tools are aimed at empowering administrators to handle their own disputes rather than setting content controls at the protocol or network level.

Because moderation is allocated in a more distributist fashion—meaning authority is nested among varying levels of communal operation—some of the tensions that arose in early internet fora operated by high-level network providers are dissolved. Unlike CompuServe or Prodigy, the Matrix protocol is not controlled by a single entity that can set moderation standards that might harm or help different parties. Rather, it is a set of rules that users and server operators abide by to participate in the network. Furthermore, as an end-to-end encrypted technology, even server operators may be limited in what communications they are able to access.[51]

The developers of the Matrix protocol state their intention to create tools that best facilitate this nested moderation, characterizing effective moderation as "the single biggest remaining risk to the long-term success of Matrix as a project."[52] They describe their three-pronged approach thus: "ensuring that moderators of chatrooms have the necessary tools to enforce whatever code of conduct they require; ensuring that server administrators can enforce terms of service on how their servers are used; [and] ensuring that users themselves are empowered to filter out content they do not wish to see."[53] Some of the tools available towards these ends include blocking and filtering mechanisms, server banning options, IP banning options, and reporting. Some of these features are necessarily limited when using Matrix's bridging technologies that allow interoperability with other communications services, as they may not be compatible.

[47] See "Clients," Matrix.org, https://matrix.org/clients/.

[48] See "Bridges," Matrix.org, https://matrix.org/bridges/.

[49] For example, "Matrix: Support for Encrypted Chatrooms · Issue #1187 · 42wim/Matterbridge," GitHub, https://github.com/42wim/matterbridge/issues/1187.

[50] "Moderation in Matrix," Matrix.org, accessed June 5, 2022, https://matrix.org/docs/guides/moderation.

[51] Guido Cornelius Shipper, Rudy Seelt, and Nhien-An Le-Khac, "Forensic Analysis of Matrix Protocol and Riot.im Application," *Forensic Science International Digital Investigation* 36 (2021), https://doi.org/10.1016/j.fsidi.2021.301118.

[52] "Moderation in Matrix."

[53] "Moderation in Matrix."

To date, the Matrix protocol has not triggered a legal liability challenge on the level of a *Prodigy* or *CompuServe* that will test the theoretical tensions between existing Section 230 jurisprudence and the operation of federated communications standards. The closest incident so far concerned private governance of content moderation policies: the Google Play Store temporarily pulled down the Element app for purported violations of user-submitted content policies, even though this app does not host any content.[54]

It seems unlikely that the Matrix project's development of tools that can assist in community-driven moderation would trigger such a challenge. However, if the project does become more popular, it is likely that some incident could initiate a legal battle.

The Urbit Ecosystem

It may be unrealistic to expect most people to "be their own servers" in the dominant computing environment as a response to the deplatforming problem. It is for this reason that many alternatives to Big Tech platforms struggle to find a user base—indeed, this is a key criticism of federated and "web3" technologies like the Matrix project.[55] It is simply not easy or intuitive to use these alternatives. The payoff is unclear and all of their friends are on large platforms anyway. Why go through the hassle of setting up a server for a network that very few people will use?

This is the problem addressed by the Urbit project. Its founder, computer programmer and homebrew political theorist Curtis G. Yarvin,[56] has characterized the project as the way one might build a networking environment if we were to start from scratch today. An early internet adopter himself, Yarvin believes that the Unix and HTTP-based internet served well the needs of the 100,000 or so sophisticated academics and researchers that constituted the initial user base. But it "doesn't scale for human beings."[57]

The Urbit platform is a personal server and clean-slate decentralized software stack. It consists of an operating function, Nock, and functional language, Hoon, that allow one's Urbit to "think." On top of these are built the operating system, Arvo, and a few in-built features: an encrypted p2p network, typed revision control system, functional build system, application sandbox, and a vault for personal files. It is a complete OS and networking environment written in 30,000 lines of code.

Crucially, your Urbit essentially condenses client and server into one unit. Each Urbit is its own server that can interact directly with any other Urbit. This is baked into the code. Users don't need to go out of their way to set up and maintain private servers for whatever needs they have. Anyone can behave as if they were sophisticated system administrators merely by booting up the Urbit.

Many benefits follow. For starters, this design affords user sovereignty. Individuals are no longer at the whim of one of a handful of large companies with one-size-fits-all policies that may be

[54] Corbin Davenport, "Google Reinstates Federated Chat App Element on Play Store after Wrongful Removal," Android Police, January 31, 2021, https://www.androidpolice.com/2021/01/30/google-pulls-federated-chat-app-element-from-the-play-store/.

[55] Moxie Marlinspike, "My First Impressions of Web3," Moxie.org, January 7, 2022, https://moxie.org/2022/01/07/web3-first-impressions.html.

[56] Curtis G. Yarvin, "Gray Mirror of the Nihilist Prince: A Portal to the Next Regime," Gray Mirror Substack, accessed June 5, 2022, https://graymirror.substack.com/; Jacob Siegel, "The Red-Pill Prince," *Tablet Magazine*, March 30, 2022, https://www.tabletmag.com/sections/news/articles/red-pill-prince-curtis-yarvin.

[57] Isaac Simpson, "Urbit and the Not-So-Dark Future of the Internet," *Vandal Press*, April 12, 2017, https://medium.com/vandal-press/urbit-and-the-not-so-dark-future-of-the-internet-400c9b667e2.

arbitrarily enforced to incentivize mostly bland, commercially friendly, or politically correct content. Data privacy issues are also addressed, as large entities no longer control mega datasets of personal data that can be leaked or cut off from users. If you don't like the policies of another Urbit, you can simply choose to not associate with them (and vice versa). Furthermore, if another Urbit decides to not associate with you, they cannot cut you off from your own data in removing their association, as is the case when a user is deplatformed by a third party and can no longer access their content and contacts from that account.

This does not imply anarchy. Usually, the flip side of a lax moderation policy is that filthy content will accrue. On Urbit, there is a cost for poor behavior. There are a limited number of Urbits that are costly to acquire. Some rarer kinds of Urbits have authentication and routing duties: these are galaxies (255 total) and stars (65,000 total). Then there are planets (4 billion total) and moons (4.3 trillion total), which can access and use the Urbit network. Each of these Urbits comes with a persistent public identity. If a user engages in trolling, criminal activity, or abuse, they will be identified and ostracized. Furthermore, they will incur a financial loss, as their reputation will be ruined. Thus content moderation problems are addressed without ill-fitting and abusable corporate or government interventions.

It is difficult to ascertain the exact user base of Urbit because of its design. The Matrix protocol seems to host tens of millions of users. As of the summer of 2022, it was estimated that 60 million accounts were registered on the network, although daily active users would be significantly fewer.[58] With Urbit, there is probably only a few thousand or so dedicated daily users.[59] As such, moderation controversies have been even more limited than on Matrix, and case studies indicating a likely path in the legal system are hard to come by.

Urbit is a virtual machine for distributed environments. It is like a browser that allows one to interact directly with other computers. As Bitcoin made it possible for individuals to send value directly to each other, Urbit makes it possible for computers to interface directly.

One can find many critiques of Urbit online. It is an ambitious project. Some believe it is too ambitious.[60] Every few years, a new project will spring forth to "rebuild the internet." Much of the web3 hype leverages this perennial quest.[61] There are many technical debates over the merits of some of the design choices. Aesthetically, Urbit is unique even when compared to other functional programming environments.[62] Yarvin describes the project as "programming for Martians," the way an alien civilization might design their networking infrastructure.[63] Critics maintain this will keep interested developers away. Ideologically, some opponents dislike the founder's right-leaning politics.[64]

[58] Richard Speed, "60 million in the Matrix as Users Seek Decentralized Messaging," *The Register*, July 15, 2022, https://www.theregister.com/2022/07/15/matrix_grows/.

[59] Mihai Grigore, "Look to the Stars: Navigating the Urbit," Messari Research, March 14, 2022, https://messari.io/report/look-to-the-stars-navigating-the-urbit.

[60] Francis Tseng, "Who Owns the Stars: The Trouble with Urbit," Distributed Web of Care, May 4, 2019, http://distributedweb.care/posts/who-owns-the-stars/.

[61] Andrea O'Sullivan, "What Is Web3 and Why Is Everyone Suddenly Talking About It?" *Reason*, November 23, 2021, https://reason.com/2021/11/23/what-is-web3-and-why-is-everyone-suddenly-talking-about-it/.

[62] Unlike every other project, in Urbit, 0 is true and 1 is false. See "2d: Bit Logic," Developers.urbit.org, accessed July 11, 2022, https://developers.urbit.org/reference/hoon/stdlib/2d.

[63] Curtis G. Yarvin, "Urbit: Functional Programming from Scratch," *Moron Lab* (blog), January 13, 2010, http://moronlab.blogspot.com/2010/01/urbit-functional-programming-from.html.

[64] Elizabeth Sandifer, "The Strange and Terrifying Ideas of Neoreactionaries," *Current Affairs*, May 30, 2022, https://www.currentaffairs.org/2022/05/the-strange-and-terrifying-ideas-of-neoreactionaries.

Can Technology Escape Policy?

Subsection (b)(3) of Section 230 states that it is a policy of the United States to "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the internet and other interactive computer services."[65] Decentralizing technologies such as the Matrix protocol and Urbit ecosystem aim to achieve precisely these ends.

The design of these decentralizing technologies, either by facilitating private server interoperability (as in the case of Matrix) or by condensing server-client functionality into one passive unit (as in the case of the Urbit), can achieve the policy goals of Section 230 without an external legal mechanism. Such designs allow for direct user broadcast and distribution without a third party onto which liability could ever fall in the first place. The issues that Section 230 tries to resolve simply do not need to exist—although, of course, such arrangements are possible in these environments as well.

These technologies should therefore be quite attractive to critics of big technology platforms who seek to achieve more user sovereignty online through the force of law.[66] Although there has been some interest,[67] we do not see significant numbers of critics turn to such alternative platforms. Mostly, the most popular critics of established technology platforms have turned to other centralized platforms such as Parler or Truth Social, which create the same technological and legal difficulties.[68]

There are many possibilities for why critics have not turned to decentralizing technologies in mass. First, most audiences are on established platforms, so there is an incentive to try to affect change on those services. Second, these alternative technologies are not particularly well known or as easy to use as a known quantity like Facebook. The decentralizing technologies that have existed for decades, such as Bitcoin, are still not often used in a truly decentralized way. Many cryptocurrency users still rely on third party services to manage and store their private keys.[69] Third, political actors have an incentive to focus on political means. A "tough on tech politician" may find her ends are best served by using a decentralized technology platform that cannot be censored, but she will get more attention and fundraising when she is "deplatformed" by an establishment actor and can channel that into more political power.[70]

Furthermore, Section 230 reform and other technology policy proposals are often intentionally wielded as a means of antitrust against large communications services.[71] Fostering and supporting an environment of decentralization and innovation may ultimately achieve similar antitrust ends, but it is not as obvious or immediate, nor are either of these two projects a certain FAANG-killer.

[65] 47 U.S.C. § 230(b)(3).

[66] O'Sullivan, "Route Around Deplatforming."

[67] Justin Murphy, "Urbit and the Telos of the Creator Economy," *Other Life*, May 27, 2021, https://www.otherlife.co/urbit/.

[68] O'Sullivan, "Route Around Deplatforming."

[69] Andrea O'Sullivan, "Bitcoin Can Fix Financial Deplatforming of Canada's Truckers—But It Won't Be Easy," *Reason*, February 22, 2022, https://reason.com/2022/02/22/bitcoin-can-fix-financial-deplatforming-of-canadas-truckers-but-it-wont-be-easy/.

[70] For example, Kevin Robillard, "Twitter Pulls Blackburn Senate Ad Deemed 'Inflammatory,'" *Politico*, October 9, 2017, https://www.politico.com/story/2017/10/09/marsha-blackburn-twitter-ad-243607.

[71] Berin Szoka and Ashkhen Kazaryan, "Section 230: An Introduction for Antitrust & Consumer Protection Practitioners," *The Global Antitrust Institute Report on the Digital Economy* 29 (2020): 1060–1117, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3733746.

Viewed from another light, the resources expended on political change carry their own uncertainties. In spite of spending many years, many more lawyers, and considerable money on antitrust enforcement against Microsoft, the government still did not prevent the company from maintaining its dominance in technology—and this is an example of a successful enforcement endeavor.

Anti-Big Tech advocates expend significant energy and resources pursuing slapdash policies against incumbents. In the case of Section 230, it is not even clear that the repeal or reform they seek would yield the intended results. Regardless, such cottage industries generally get paid.

If the policy future of Section 230 reform seems uncertain, the opening for new laws to restrain a successful decentralized networking environment are a good bet. This has been the case with the cryptocurrency industry, which has seen many proposals for new laws and regulations to restrain peer-to-peer commerce.

Assuming that projects like Matrix or Urbit take off and users are imbued with more sovereignty online, other platforms and governments will surely take note. Already, Mastodon clients have been temporarily deplatformed for violating Google's user-submitted content policies, even though such apps host no user content and therefore could not be in violation of such rules (the apps were eventually reinstated).[72] So far, such apps are relatively small, and have not attracted much notice. Should they continue to grow in popularity, so too will the urge to constrain such peer-to-peer communications.

Like with Bitcoin, however, decentralization limits the possibilities of policy. Fewer large third parties to target means more legwork for enforcement. Government agents must find and identify individuals involved with each incident. There are no single clearinghouses that can be captured and controlled.

Perhaps decentralization technologies will not attain a critical mass of users to warrant such high-level attention. In this case, we could see a kind of two-tiered internet environment where savvier or more sovereignty-minded individuals wield decentralizing technologies for more direct control while most users continue to use large technology platforms that are mostly sanitized and controlled for commercial and political ends.[73]

Whatever the scale, the emergence of stable decentralized networking environments should cast many of the unspoken contours of contentious technology policy debates—such as Section 230—in sharp relief. Roundabout distinctions between editorial and distributional functions suited to earlier days of mass broadcast will likely fall to the side in favor of more direct conversations over permissible speech and user sovereignty.

[72] Andrea O'Sullivan, "Innovators Are Crafting Decentralized Social Media Alternatives. Will App Stores Pull Them Down?" *Reason*, September 9, 2020, https://reason.com/2020/09/09/innovators-are-crafting-decentralized-social-media-alternatives-will-app-stores-pull-them-down/.

[73] Andrea O'Sullivan, "Preparing for a More Fractured Web," *The Journal of the James Madison Institute* (Fall 2020): https://www.jamesmadison.org/wp-content/uploads/2020/10/Journal_06_Fall2020.pdf.