International Journal of Communication 18(2024), 5607-5628 1932–8036/20240005

Can This Platform Survive? Governance Challenges for the Fediverse

THOMAS STRUETT
ARAM SINNREICH
PATRICIA AUFDERHEIDE
American University, USA

ROBERT W. GEHL
York University, Canada

In the wake of recent crises at commercial social media platforms like Twitter and Reddit, the "fediverse" has gained adoption and visibility as a noncommercial alternative for individuals, communities, and institutions to develop channels of public communication, dialogue, and debate. In this article, we draw on illustrative examples from the history of digital civic discourse and identify 6 ways in which history shows us how the potential benefits of the fediverse are at risk of subversion. We discuss several potential threats to these spaces of civil discourse, including challenges inherent to distributed governance, commercial platform capture, inclusive access, moderation at scale, reputational assaults by commercial competitors, and the neoliberal technoromanticism familiar from previous digital innovations. These threats must be addressed collectively and proactively by key fediverse stakeholders in an ecology whose ruling values are noncommercialism, decentralization, open source, free association, and wariness of traditional governance.

Keywords: federated social media, platform governance, social media, Mastodon, alternative social media

In the wake of recent high-profile crises at commercial social media platforms such as Twitter and Reddit, the "fediverse" has gained adoption and visibility as a viable noncommercial alternative for individuals, communities, and institutions to develop channels of public communication, dialogue, and debate. In this article, we draw on illustrative examples from digital civic discourse and identify six ways in which its history demonstrates how the potential benefits of the fediverse are at risk of subversion, either by commercial competitors or through structural dysfunction.

Thomas Struett: ts9386a@american.edu
Aram Sinnreich: aram@american.edu
Patricia Aufderheide: paufder@american.edu
Robert W. Gehl: rwg@yorku.ca
Date submitted: 2023-09-29

The fediverse is a decentralized, open-source, largely nonprofit ecology of bounded, linkable social media sites, apps, and services (e.g., Mastodon, Pixelfed, Lemmy), built on the ActivityPub social web protocol. Many users who constituted Twitter's (now X) most active noncommercial communities—academics, journalists, artists, minoritized intellectuals, activists, and technologists—have turned recently to the fediverse, to reestablish collegial networks of information sharing and cultural exchange.[1]

Community-specific servers (or "instances") hold promise as democratically run platforms for civil discourse within and between these groups of users. Because each instance may federate—interlinking with other individuals and instances—the fediverse could, potentially, become a mass-scale network of smaller networks foregrounding trust, integrity, and information quality.

The fediverse's early years have been marked by utopian enthusiasm, volunteer labor, goodwill, and ad hoc sharing, as is common in burgeoning open-source and noncommercial online spaces (Cabello, Franco, & Haché, 2013; Mansoux & Roscam Abbing, 2020; Sevignani, 2013). There is no reason to assume this will continue, as millions of new users "migrate" from commercial services. Communication platforms are always susceptible to cycles of co-option (Wu, 2010), and many platforms sacrifice their civic and communal value over time, becoming "enshittified" in the pursuit of profit (Doctorow, 2023).

In this article, we discuss potential threats to federated spaces of civil discourse, including challenges inherent to distributed governance, commercial platform capture, inclusive access, moderation at scale, reputational assaults by commercial competitors, and neoliberal technoromanticism. These threats must be addressed collectively and proactively by fediverse stakeholders in an ecology whose ruling values include noncommercialism, decentralization, open source, free association, and wariness of traditional governance.

The fediverse's technological foundations cannot solely guarantee the existence of robust and decentralized civil discourse via social media. Developers, entrepreneurs, institutions, and users must also work to avoid these historical threats and maximize the fediverse's civic potential.

Commercial Social Media vs. the Fediverse

The inherent tension between commercial social media's user-friendliness and its exploitative capacity, and the constantly negotiated space of agency for users between the two, has contributed to recent disruptions in the sector. Facebook has seen growth stall and brand tarnishment since the Cambridge Analytica scandal (Vogels, Gelles-Watnick, & Massart, 2022). TikTok has been widely denounced (reasons range from legitimate cybersecurity concerns to outright xenophobia) as a tool for Chinese-state surveillance and propaganda (Mueller & Farhat, 2023). Reddit users have quit *en masse* after the company faced off

[1] It is difficult to measure the size of the fediverse because it is noncentralized. Several projects track it: https://fedidb.org/, https://fediverse.party/en/fediverse/, https://the-federation.info/, and https://mastodon.social/@mastodonusercount. Each varies, because each observes different sets of servers. All reflect explosive growth in accounts during 2022–2023. Since then, users have dropped but remain far above historical levels. In October 2021, the fediverse had ~about 4.1 million accounts (Gow, 2022). Today it is about 14 million.

against its own moderators and developers over collecting user data for AI development (Field &Vanian, 2023). And Twitter—rebranded in mid-2023 as X—has seen cascading outages, advertiser abandonment, user loss, and brand tarnishment since its acquisition by Elon Musk (Mac & Hsu, 2023). Although some commercial competitors have exploited this market vacuum (for instance, Meta's Twitter-like Threads service), millions of users have also investigated the fediverse as a potential alternative for large-scale online communities.

The "fediverse," or the universe of federated social media, is a network of servers running social media software that enables each server to communicate with any another (Roscam Abbing, Diehm, & Warreth, 2023). Since 2008, there have been various technical approaches. Today, the most popular involves a standardized protocol called ActivityPub (Lemmer-Webber, Tallon, Shephard, Guy, & Prodromou, 2018).

Users on a given server are able to reach other users on other servers across the network. For instance, if user1 is on serverA, running Mastodon (a microblogging platform) and user2 is on serverB, running Pixelfed (a photo-sharing platform), each may follow the other to see, like, and comment on their posts. Much as open-source e-mail protocols allow users to send e-mails to each other from different services (e.g., Gmail and Hotmail), ActivityPub allows users of different fediverse services to send social media data to one another. The result is a noncentralized technical infrastructure (Gehl & Zulli, 2023), distinct from the centralized corporate social media model.

The fediverse is more than a technical system; it is also a political structure (Mansoux & Roscam Abbing, 2020). Administrators and users on these services must decide whether or not to federate with other users and servers. For example, if a server dedicated to White supremacy or child exploitation appears on the network, the rest of the fediverse may block that server—a situation that happened in 2019 when countless instances blocked the ActivityPub-based alt-right social media service Gab.com (Caelin, 2022).

Conversely, many fediverse administrators seek to federate with like-minded communities, based on values embodied in their "codes of conduct." Gehl and Zulli (2023) call this "covenantal federalism," a democratic political network based on a shared set of values. Thanks to social and practical choices made by early Mastodon developers and admins, thousands of connected fediverse instances now use similar codes, prohibiting actions such as hate speech and harassment and encouraging local, human moderation and collective decision making.

This fusion of technical decentralization, locally oriented governance, shared values, and standardized protocols results in a large network of small, interconnected communities. Each server may be small (most have fewer than 500 users), but the resulting network is large and global.[2] Thus, the fediverse's sociotechnical affordances include new potential for civic engagement via social media. Millions of people, including journalists, artists, academics, politicians, and nonprofits distribute and discuss news, politics, and culture via the fediverse. Thus, they are engaged in the positive, civic-minded practices sometimes

[2] Per fediverse.observer, in August 2024 there are about 21,000 servers worldwide. Thus, the average server has about 600 users. However, 75% of servers have fewer than 10 users and only 3% of servers have more than 1,000 users.

associated with corporate social media, but without necessarily inheriting many of the problems posed by centralized systems (e.g., algorithmic manipulation, widespread disinformation, and the commercialization of sociality).

There are no guarantees this federalized network of small, locally operated social servers running on an open protocol will remain viable, democratically controlled, or ethical. Effectively, the fediverse has three key modalities of governance, each with unique practices and needs. One is the W3C standard ActivityPub protocol, which maintains and extends that standard. Another is the maintenance and development of fediverse software packages, such as Mastodon, Pixelfed, and Lemmy. Finally, there is the governance of specific fediverse instances, which involves internal content moderation as well as diplomatic relations between instances.

As scholars of science and technology studies (STS) and Internet governance have long held, the social adoption and maintenance of technological innovation is a complex process that involves multiple "chokepoints" (DeNardis, 2020; Giblin & Doctorow, 2022), each of which creates an opportunity for stakeholders to shape or constrain the use of technology at a large scale, with global cultural and civic consequences. Similarly, as scholars like Caplan and Gillespie (2020) and Gorwa and Ash (2020) have demonstrated, the structure of platform governance and moderation is both reflective of and integral to the functioning of democratic processes in digital networks, and much of the proverbial "devil in the details" comes down to arcane and obscure questions about transparency, control, and information flow at any given chokepoint or sociotechnical layer. With several modalities of fediverse governance, there are many chokepoints and details to consider.

In addition, the struggle for democratic governance over digital civic platforms is not only internally complex, it is also subject to exogenous factors. The dominant business model for social media has been an extractive process of data profiling, which has been variously termed "surveillance capitalism" (Zuboff, 2019), "platform capitalism" (Srnicek, 2017), and "data capitalism" (West, 2019). This system is intertwined with neoliberal political philosophies, advanced by "big tech" lobbyists, premised on limiting the capacity of government regulation (e.g., data privacy, antitrust, or AI policy) to protect the ability for publics to form in the Deweyan sense (Dewey, 1927). Finally, as scholars including Gibson (2023), Phillips and Milner (2021), and Roberts (2019) show, both the unpaid work of users and volunteers, and the poorly paid work of professional content moderators, further exacerbate the extractive relationships between commercial platforms, users, and workers, and present challenges to scale in noncommercial networks like the fediverse.

Taking these theoretical frameworks and sites of research into account and drawing on our own review of analogous historical efforts to build spaces for civic discourse, democratic deliberation, and decentralized governance on the Internet, we have identified six potential threats to the continuing viability of the fediverse that we outline below.

Six Potential Pitfalls for the Fediverse

Distributed Governance Failures

Previous decentralized platforms have sometimes failed to deliver on their civic potential because of challenges emerging from governance: the norms, institutions, and technologies that determine who gets to say what to whom and under which circumstances. In addition to users and platform operators, such decisions may be made by developers, political actors, advocacy groups, and researchers (Gorwa, 2019).

Though corporate platforms emulate traditional media structures by centralizing power (Napoli & Caplan, 2017), the fediverse has a more distributed governance structure. This decentralization is not just an aspect of the underlying software but also a core tenet of its governance philosophy. This model also differs from alt-right platform governance (Gehl & Zulli, 2023), because of the unique use of codes of conduct. Although decentralized governance can help avoid some of the pitfalls associated with commercial and alt-right platforms (for instance, limiting corporate capture and political censorship), it introduces other risks that must be addressed and mitigated, including new threats such as accountability and liability crises, forking, and security vulnerabilities. Corporate actors may also exploit these challenges by posing themselves as solutions to distributed governance frictions (Marshall, 2006).

Historical examples of distributed governance challenges are legion. Because so many essential building blocks of social platforms emerge from the free software and open-source communities, leadership and ownership vacuums tend to emerge around specific software tools and protocols, especially older and more established ones, where development has slowed or ceased altogether (Sinnreich & Gilbert, 2024). This is what happened in the case of Log4J (Gülcü, 2001), an open-source tool managed by the Apache Software Foundation that is used to record activity within software. In 2021, over two decades after Log4J was developed, it was discovered to have a critical security vulnerability, rendering the hundreds of millions of software platforms, services, and devices that depended on it vulnerable, as well (Starks, 2021). Once the vulnerability was revealed to the Apache Foundation, it rushed to patch it (Turton, Gillum, & Robertson, 2021). Nonetheless, the flaw remains "endemic" because Log4J is embedded into many larger software systems, making it difficult for organizations to become aware they are running a piece of vulnerable software (Suderman, 2022).

Another challenge in distributed governance is the tendency for projects to "fork," when changes made to a project's root code are adopted by some developers but rejected by others, creating a situation in which two different, and increasingly incompatible codebases are developed in parallel. A good example of this is the forking of OpenOffice. OpenOffice was a suite of word processing, spreadsheet, and presentation apps maintained as an open-source software (OSS) project by Sun Microsystems during the 2000s.

The OSS community was dissatisfied with Sun's development processes and with the requirement that coders assign copyright for their work to Sun (Paul, 2010a). In 2009, Oracle acquired Sun, spurring OpenOffice developers to adopt community-driven governance of the project. In 2010, many of them started a nonprofit, The Document Foundation (TDF), to maintain a fork they called LibreOffice. Oracle told developers that participation in both projects was a conflict of interest and required them to pick a side

(Paul, 2010b). Most moved to LibreOffice, and in 2011, Oracle stopped developing OpenOffice and ceded the project to the Apache Foundation. Five years later, there were 250 active developers working on LibreOffice and only four on OpenOffice (Corbet, 2015).

Another potential vulnerability is corporate subversion of distributed governance systems. OSS can involve many developers contributing asynchronously and globally. Corporations see cost savings and other benefits from tapping into this system and often participate in OSS development. However, commercial actors can also exploit these systems by directing projects toward their own ends.

An example of this corporate subversion is when the World Wide Web Consortium (W3C) approved the Electronic Media Extensions (EME) standard in 2017. EME allows browsers to play back encrypted media. Critics expressed concern that copyright law could be used to prosecute researchers who work to expose bugs in browsers using EME (Doctorow, 2017). EME also requires browsers—even open-source ones—to license proprietary software from Google (Doctorow, 2019), increasing development costs and limiting the use of OSS development. Hill (2018) describes this corporate capture of OSS projects as "strategic closedness."

In short, distributed governance can open vulnerabilities by creating accountability gaps within nested dependencies, a lack of hierarchy can lead to incompatible and inefficient software forks, and corporations can use their vast resources to subvert open-source development toward their own needs, often at the detriment of user autonomy and developer independence.

There are many ways in which these challenges might pose pitfalls for the fediverse. For example, instance administrators maintain codebases that must be updated continuously to secure against undiscovered vulnerabilities. As the example of OpenOffice shows, distributed governance can lead to duplication of such tasks. In the case of the ActivityPub protocol or the Mastodon code, efforts to address core vulnerabilities could cause fractures in the fediverse as users and administrators decide which software fork to follow.[3] Truth Social, founded by Donald Trump, is an example of a Mastodon code fork. The site's developers chose not to federate with the rest of the fediverse and violated Mastodon's free software licenses (and, by extension, U.S. copyright law) by keeping their forked code private (Clark, 2021). Corporate subversion of ActivityPub governance is also a potential threat, especially since Meta launched its ActivityPub-based Twitter competitor, Threads, in 2023 (Barber, 2023).

Commercial Capture

Another challenge that has undermined previous decentralized and open platforms is commercial capture. Proprietary, value-added features enhancing the user experience are used to bring more users onto the platform, to retain them as customers, and to encourage them to share more data to generate profit. Such features have included news feed algorithms, enhanced one-to-one communication tools, identity verification, rich media affordances, and customization tools, driving "behavioral surplus" (Zuboff, 2019).

[3] This is a hypothetical scenario. To date, security vulnerabilities that have been found in the Mastodon codebase have been dealt with quickly and uncontroversially (Jones, 2024).

There are many instructive examples of commercial capture on earlier open platforms. One such example is e-mail. All e-mail services rely on open-source protocols such as POP, IMAP, and SMTP. Yet e-mail has become increasingly centralized and commercialized and is used as a linchpin of integrated platform capitalism strategy. An example is Google's Gmail service. Google attracted its user base of more than 2 billion monthly active users (Fried, 2020) by adding value through search functionality, optimized user interface, increased storage, and guaranteed free access. At launch, its gigabyte of free storage space was unheard of among competing e-mail providers (Boutin, 2004). But although promising users that they would never have to delete an e-mail again and encouraging them to think of Gmail as a personal archiving service, Google also mined the text of users' e-mails to deliver targeted advertising and build detailed user profiles across its broader suite of services and platforms.

After attracting users to a service, corporate capture continues through the creation of "walled gardens"—ecosystems built to retain users and disincentivize them from deleting their accounts or switching to competitors. AOL's proprietary publishing software RAINMAN (remote automated information manager) is an example of this walled garden approach. From the early 1990s to the early 2000s, all AOL content and advertisements had to be programmed in RAINMAN. RAINMAN was useful because it was optimized for a seamless experience at dial-up Internet speeds. Publishers and advertisers were incentivized to develop with RAINMAN because it gave them access to AOL's large user base. But after the mid-1990s, HTML (hypertext markup language), the open-source Web development language, allowed for more dynamic content and advertisements to be created and allowed publishers and advertisers to reach users beyond the AOL walled garden. This ultimately diminished the value of developing exclusively for RAINMAN and eventually contributed to the open Web overtaking AOL as a destination for online users (Walker, 2004).

This example is instructive because it shows that the power of commercial capture can be limited by developments in a robust open-source community. On the other hand, commercial platforms can defend against the erosion of their dominance by erecting stronger barriers to prevent users from switching, employing both proverbial carrots (value-added features) and sticks (preventing users from exporting their own data).

The ActivityPub protocol, like HTML, is open source and highly interoperable. However, this will not necessarily prevent commercial capture of the fediverse. Arkko and colleagues (2019) describe this as the "Permissionless Completeness Problem" (p. 7). If an underlying network protocol like ActivityPub is powerful enough, applications built on top of it can become sufficiently complex to support closed-off services. Thus, only a continuing commitment to interoperability by developers, and not merely the existence of an open technological standard, can ensure an open ecosystem within the fediverse. As commercial social media services like Tumblr and Threads begin federating via the ActivityPub protocol, it is instructive to observe how they use value-added features like celebrity seed accounts (Heath, 2023) and single sign-on (Mehta, 2023) to keep users within their walled gardens, disincentivizing users, and publishers from switching to federated noncommercial alternatives. Communities on the fediverse are already pushing back with initiatives like FediPact, where around 800 instance admins have agreed not to federate with Meta's fediverse alternative (Barber, 2023).

Access Issues

Ease of access for users and communities is essential to the inclusiveness—and, therefore, the viability—of the fediverse ecology. Anecdotally, the greatest obstacle to joining the fediverse is that people do not understand how, despite news articles and how-tos written to address this confusion (Butler, 2022). The nonprofit behind Mastodon has acknowledged that this is a major barrier to access and has simplified the onboarding process by defaulting new users to its own instance (mastodon.social). This points to another threat in which the rhetoric of "user-friendliness" can mask a reduction in user agency.

Accessibility challenges are often discussed via a "digital divide" framing (Hawkins, 2005), but there are other obstacles and consequences to consider as well. For instance, another common barrier to platform accessibility is gatekeeping (Driscoll, 2023), in which established users employ techniques such as norms policing and technical jargon to challenge the validity and limit the participation of new users, disincentivizing adoption. Gatekeeping has already been observed on the fediverse, and is listed as a reason that some vibrant social media communities (such as "Black Twitter") have yet to embrace it fully (Hendrix & Flowers, 2022).

A historical example of gatekeeping through norms policing is known as "Eternal September." In the 1980s and early 1990s, each September, Usenet (an open platform for online interest groups) was flooded with new users because college students would start adopting the platform. These newbies were often looked down on by established users for breaking unwritten norms or merely for requesting advice. "Eternal September" refers specifically to February 1994, when AOL allowed all of its users to access Usenet, inundating the platform with newbies and sparking frustration, outrage, and backlash among established users. Driscoll (2023) argues that longtime Usenet users were not necessarily objecting to the influx but rather more generally to the increasing accessibility of the Internet, diminishing the "special status afforded to 'real' Internet users" (para. 13). The lesson for the fediverse from Eternal September is not that new users must be taught the social norms of the space they are joining, but that norms policing is a form of gatekeeping that can exclude new and more diverse users from joining.

When digital platforms have influxes of new users, they will typically need to scale moderation quickly to deal with the greater volume and diminished expertise of these user bases. For example, Wikipedia dealt with an influx of new contributors in the mid-2000s. To moderate the unprecedented volume of contributions, automated moderation tools were adopted, entrenching norms and discouraging newcomers from becoming editors. As Halfaker, Geiger, Morgan, and Riedl (2013) demonstrate, the detached and impersonal style of automated moderation tools and the binary choice they offer between rejection and acceptance limit nuance and negotiation, making it harder for newcomers to participate equally. Therefore, automated moderation may be understood as a form of sociotechnical gatekeeping.

Technical language or knowledge may also be used to limit access to the fediverse. Gehl (2016) identified the ethic of "techno-elitism" in the Dark Web Social Network (DWSN) that is only accessible through Tor-enabled browsers. DWSN administrators described how a working understanding of Tor is used "as a sort of 'admissions test' one must pass before being seen as competent in helping build the DWSN community" (Gehl, 2016, p. 1228). Although the DWSN would be more accessible via Google search or

Wikipedia, existing users restricted those options, further limiting accessibility. Those who lack the knowledge of how to join are labeled as "lazy" or "incompetent," creating a power dynamic between the "technical elites" on the DWSN and open-Web users. Such gatekeeping ensures that new adopters will closely resemble existing ones. It also slows growth, making moderation more manageable. However, it also prevents most people from enjoying the very freedoms the DWSN community prides itself on.

"User-friendliness" may also constrain user autonomy, setting a power differential between developers, expert users, and everyday users of a platform. Black (2022) demonstrates that user-friendliness emerged from an ethic of expediency by technological elites. Usability is often promoted as "democratization" because it makes technology accessible to more people. Pushback by users seeking stronger agency over technology is disparaged as a form of techno-elitism. However, making a technology more user-friendly often obscures and reifies commercial values, such as centralization, within the architecture of a platform.

For instance, Black (2022) demonstrates how hobbyists of the 1970s who promoted decentralized "personal computing" in contrast to centralized IBM mainframes realigned their values when it came to usability. Many hobbyists supported proprietary software because they believed its higher usability justified abandoning open-source development. Black argues this ethic of expediency prioritized technological concerns (usability) over political and cultural ones (democracy, user agency). Although the personal computer decentralized computing, user-friendliness recentralized it.

In sum, access to emerging social platforms can be hampered through gatekeeping via both norms policing and automated moderation tools. Techno-elitism expressed through technical language and expertise requirements may compound these obstacles. A *friendliness paradox* also arises when barriers to entry are removed, making the platform easier to join and use, while also limiting users' agency to make choices about the underlying infrastructure that will best foster their communities.

The fediverse faces similar potential vulnerabilities. It has already developed a disproportionately tech-savvy core user base. With an influx of users from Twitter, Reddit, and other commercial services, some have described 2022–2023 as the fediverse's Eternal September, whereas others refer to it as a "trial by fire" because of new users' disregard for existing norms (Smith, 2022). Slipups and technical misunderstandings are already used to shame users (Dunbar-Hester, 2024; Smith, 2023). When users complain about antisocial behavior they witness or are subjected to, others may shift the burden onto the victims of these interactions, telling them to go create their own instances—what Johnathan Flowers refers to as the "rugged individualism" ethic of the OSS community (Hendrix & Flowers, 2022).

In an effort to overcome technical hurdles to access, Mastodon has made one instance the default instead of forcing newbies to choose an instance immediately (Rochko, 2023). The organization argues that the only way for Mastodon to become mainstream is to make it easier to access for those who are not motivated primarily by the promise of decentralization. As Mastodon creator Eugen Rochko stated in an interview with one of the authors, shunting new users to Mastodon.social gives them a "more or less traditional social media service that you'd expect."

Alternatively, Rochko recommended new users start their own instances of one, where they would be "completely in control. It's like running your own blog. Nobody can dictate what you can and cannot say, how you should behave, who you should talk to." He argued against new users joining midsized servers. "For a person coming from outside the fediverse, that's not necessarily the best choice for them to start on" because midsized servers have "inter-server politics" and "drama" that can degrade the new-user experience.

Per the friendliness paradox, this move to make onboarding more "friendly" might limit the autonomy of users: either they join a large server, or they run their own; they are advised against getting involved in "inter-server politics." Although this might make the fediverse more user-friendly, it prevents new users from learning how small communities self-govern and may result in de facto network centralization. We do not see any reason to believe this paradox will be resolved in the fediverse more effectively than on any other platform.

Moderation Conundrums

Moderation is a core aspect of any social platform (Gillespie, 2018). However, moderation is the greatest vulnerability both to the business model of a platform and to its utility as a civic space. The fediverse offers tools like individual blocking, instance blocking, and codes of conduct for moderation. Codes set expectations about how users behave toward others and are important for expressing the values of an instance (Gehl & Zulli, 2023). The decentralized nature of the fediverse has also made the labor of content moderation more visible to users and administrators by localizing it within individual communities (though resources like block lists are often shared across multiple instances). This introduces equity challenges to the fediverse with a disproportionate burden of moderation labor falling on communities that are more likely to be harassed (Hendrix & Flowers, 2022). Vulnerabilities stemming from moderation include the difficulty of scaling, matching moderation to community values, and placing moderation as an afterthought in the creation of a civic space.

As users of a social network grow, so must the cost of moderation. This leads to most commercial networks underinvesting in moderation. The consequences of this decision can be seen in the case of Reddit. Content on Reddit is divided up into "subreddits" that revolve around specific topics, hobbies, or issues. Each subreddit is moderated by a group of volunteers who are a part of the community. The value of labor done by these unpaid volunteer moderators has been estimated conservatively at $3.4 million a year (Li, Hecht, & Chancellor, 2022). In 2015, after the unexpected dismissal of a Reddit employee seen as essential by many volunteer moderators, more than 2,000 subreddits joined a blackout to call on Reddit staff to improve communication with these volunteer moderators and improve software tools for community moderation (Matias, 2016). This protest resulted in the departure of the company's CEO and the creation of a CTO position focused on building software for volunteer moderators.

Moderation must also confront the irreconcilable values of diverse users. The fediverse and Reddit approach this challenge similarly, prizing smaller communities of instances or subreddits establishing their own rules. This gives users the choice to exit when they disagree with a community's norms, and in the case of Reddit, contributes to a libertarian stance on free speech (Grimmelmann, 2015). Historically, Reddit

moderators have often removed content deemed inappropriate, but then faced backlash from the wider user base for ostensibly trampling on free speech. This has happened with respect to child pornography (Reddit, 2012), White supremacism and body shaming (Abad-Santos, 2015), and pro-Trump messaging (Fischer, 2020). Thus, despite Reddit's emphasis on self-governance, there are still continual battles over moderation.

The relationship between Reddit and moderators reached a crisis point in 2023 when the company updated its application programming interface (API) deliberately to prevent third-party commercial services from exploiting free access to user posts (Wiggers, 2023). Many volunteer moderators also relied on these third-party services to help them manage their labor. Thus, many subreddits "went dark" to protest what they perceived as a calculated profit-oriented decision that ignored their needs. In short, Reddit's underinvestment in supporting community moderation contributed to a large-scale exodus of users (and volunteers) from the platform.

Moderation challenges pose a real threat to the fediverse. Moderation costs do not scale with platform growth. Human moderation is labor intensive. And although automation can lower costs, it does not function well with nuance, which can increase liability costs and exposure to platform abandonment. Moderation practices must also be revised continually to reflect changing social values and technosocial affordances. Because of these challenges, moderation often becomes an "afterthought" (Gillespie et al., 2020) for quickly growing services. Fediverse developers and instance operators, seeking to accommodate large volumes of users leaving commercial platforms, may choose to prioritize growth over good moderation.

Rochko's decision to make Mastodon.social a default instance has been criticized by other fediverse admins, who argue that such a large instance cannot be well moderated, and who tend to prioritize moderation quality over user growth (Gow, 2022; Mansoux & Roscam Abbing, 2020; Zulli, Liu, & Gehl, 2020). However, even within smaller instances, the challenge of scaling moderation resources will remain; although the fediverse currently relies on the goodwill of countless volunteer moderators and self-funded instances, this goodwill cannot last indefinitely, and a workable approach to funding and compensation has yet to emerge.

Reputational Antihalo

A platform's reputation may be damaged by association with the actions of a few unsavory adopters. In crisis communication, a "reputational halo" refers to a brand's prior reputation protecting it from damage during a crisis (Coombs & Holladay, 2006). Here, we propose the reputational "antihalo." This refers to the negative reputation that a whole suite of technologies may accumulate from their antisocial or illegal use by a subset of users. Historically, entrenched commercial interests have exploited such negative associations against new and emerging technologies (especially free, open-source, and decentralized software) when they threaten their market dominance.

For instance, Sinnreich (2013) demonstrates how the music industry framed decentralized, peer-to-peer (P2P) file-sharing technologies as "piracy" tools. Like e-mail, the World Wide Web, or the fediverse, P2P is not one specific technology but a suite of codes, protocols, and architectures that allow two or more users to share information in various contexts. Nonetheless, shortly after the summer of 1999, when Napster

launched, the music industry began to scapegoat P2P writ large as a piracy haven and as the greatest single threat to musicians and music industries. Following a multiyear, multimillion-dollar "public awareness" campaign by the major labels, the news media universally adopted the inaccurate frame that file sharing was the sole cause of the decline in record sales during the 2000s. In fact, dozens of empirical studies fail to show any consistent relationship between P2P and music revenues (Sinnreich, 2013).

Although the recording industry's "public awareness" campaign technically ended in 2008, the industry continues to maintain the "piracy" rhetoric about P2P, and most media coverage replicates this uncritically (even though, in 2023, despite or because of online free distribution, the industry garnered record high revenues; Music & Copyright, 2023). This reputational antihalo still lingers over P2P technologies today and has likely limited further investment and development of the underlying technology for civic purposes.

The reputational antihalo is not unique to P2P. It can be seen across a wide swath of technologies that potentially threaten the entrenched power of existing institutions. Tor and the "dark Web" are often labeled as havens for drug dealing and child abuse, even though they also have many civically beneficial uses like preserving freedom of expression in oppressive regimes (Gehl, 2016). And end-to-end encryption, an algorithmic means of shielding communications from surveillance, has been associated widely with threats of terrorism and child abuse (Opsahl, 2021). Although P2P, Tor, and encryption may certainly be used toward criminal and harmful ends (like any other technology), these campaigns can be understood as exemplars of "moral panics" in which the perceived threats are exaggerated by powerful interests for social control (Hall, Critcher, Jefferson, Clarke, & Roberts, 1978). The reputational antihalo is already cropping up in discourse about the fediverse and Mastodon, which have been tainted by their uses among the "alt-right" (Makuch, 2019) and for child abuse (Thiel & DiResta, 2023).

Technoromanticism

New technologies are often viewed through rose-colored glasses. For both naive and cynical reasons, they are presented as liberatory, utopian, and even as a panacea for the intractable challenges of the human condition. As history demonstrates, "technoromanticism" (Coeckelbergh, 2017; Coyne, 1999) frequently involves three fallacious tropes that present challenges to the civic utility of new communications platforms:

1) That new technologies will liberate humankind from labor, suffering, or even mortality. This deterministic view obscures the necessary social and political actions needed to capitalize on technology's liberatory capacity, and in so doing, discourages adopters, technologists, and lawmakers from undertaking these necessary actions.

2) The "great man" trope, presenting new technologies as the unique achievements of singular individuals. This view obscures the vital role of institutions and communities in the development and maintenance of technology.

3) Equating market success with social utility, downplaying the importance of government regulation, and shifting the gauge for social progress from collective political liberation to individual economic liberty.

Technoromanticism has been evident in many previous eras. For instance, Streeter (1987) examines how utopian hopes for cable television undermined its future. Claims for the diversifying, democratizing, and culturally enriching potential of the platform, as well as a technologically deterministic framing of its effects, contributed to a lax regulatory approach to the industry. Thus, large cable networks were able to maintain a powerful and highly consolidated position. As Carey and Quirk (1970) argue, the dream of "electrical utopia" is often exploited by legacy institutions as a screen for entrenched power and to ward off government regulation and market competition. And as Sinnreich, Aufderheide, Clifford, and Shahin (2021) demonstrated in the case of "Web 2.0" technoromanticism, these utopian discourses about new technologies are soon replaced by more utilitarian ones when their disruptive potential has been exhausted.

Technoromanticism is also often associated with the "great man theory" (Corbett & Spinello, 2020), which ascribes technological innovations and industrial achievements to singular individuals while overlooking the systems, institutions, and collective actions that surround them. Streeter (2010), for instance, shows how a romantic individualistic narrative of OSS as the achievement of devoted individuals liberated from corporate bureaucracy obscures the other institutions necessary for its success. For example, Linus Torvalds, known for his development of the Linux Kernel, has stated he would not have had the freedom to program Linux for no pay without his basic needs being met by the Scandinavian welfare state. As Streeter argues, technoromanticism works to obscure the collective effort that is key to technological development, undermining support for the policies that nourish such effort.

Another technoromantic trope is that new digital technologies eliminate friction in communication and boost productivity, a rising tide that floats all boats. Yet although new technologies may remove some frictions, they introduce others, and in so doing, obscure social inequalities and power imbalances behind a sheen of efficiency. Meta's rhetorical use of "connecting the world," for instance, conceals the profit motive inherent in building a social graph (Hoffmann, Proferes, & Zimmer, 2018), and introduces disinformative "bullshit" (John, 2019, p. 3) into the quest for intercultural and international understanding. In the case of the Arab Spring, Mejias (2012) shows how utopian, technoromantic discourses about social media platforms helped to circumvent discussions on the underlying market structures of digital platforms and their role in the democratic process. Mejias (2012) further argues that the commodification of social labor, privatization of social spaces, and surveillance of dissenters enabled by these networks work against the purported democratizing "effects" of social media.

The fediverse is particularly vulnerable to technoromanticism. It is often cast as inherently democratizing because of its uniquely federated architecture, yet there is nothing preventing commercial capture at a large scale. Therefore, its future is contingent on the political will of developers, admins, users, and regulators to harness its civic potential. The fediverse is also vulnerable to the individualism associated with technoromanticism. For instance, new users of the fediverse who cannot find a safe and welcoming social space are often enjoined to create their own instances (Hendrix & Flowers, 2022). This framing obscures the responsibilities that communities and instances have toward one another and ignores the vast

array of elements and stakeholders that are necessary to maintain a functional online civic space. Last, these utopian visions and individualism are premised on the viability of market-based solutions to social problems. Yet these solutions tend to be extractive and disempowering to the communities that would most benefit from a civically functional fediverse.

Conclusion

The fediverse faces several threats as a viable civic space for users and social institutions. In this article, we describe six of these potential pitfalls, drawing on historical analogy and contemporary scholarship to provide administrators, developers, and end users with the context to address these vulnerabilities proactively. We do not present this list as exhaustive or comprehensive, but do believe it can help serve as a starting place for productive planning to maximize the civic potential of decentralized social media.

Vulnerabilities resulting from *distributed governance failures* originate both from within and outside the governance structure, contributing to accountability gaps and increasing the threat of code forking, in addition to the potential for corporate subversion of governance. *Commercial capture* can also diminish the civic value of the fediverse. For instance, value-added services may be added to open-source standards and platforms to attract users and then used to erect "walled gardens," capturing users within proprietary spaces that are both extractive and difficult to exit.

We also identify several potential *access issues*, which are practices and protocols that can alienate or exclude users, especially those occupying minoritized and structurally disadvantaged social positions. Gatekeeping may be used knowingly via norms policing to prevent newcomers from joining and unknowingly via automated moderation practices adopted to help underfunded instances scale with growth. Technical language and the requirement of baseline technical expertise may also present unintended obstacles to adoption. Conversely, the rhetoric of "user-friendliness" may threaten user agency or justify recentralization of the network.

Moderation conundrums are the threats and vulnerabilities presented by the labor-intensive, messy, and continuous practice of maintaining a healthy and inclusive space for civic discourse. Although the fediverse has largely relied on volunteer moderation labor and presumptive goodwill among new users, these will not prevent the platform from facing the same challenges that have plagued centralized, commercial alternatives: a scylla-and-charybdis choice between expensive and traumatizing human moderation on the one hand, and dehumanizing, biased, automated moderation on the other.

There are also discursive threats to contend with. For instance, ActivityPub is vulnerable to a *reputational antihalo*, a term we use to represent the brand tarnishment-by-association that a technological standard can suffer because of the actions of a subset of users. This vulnerability may be exploited (as it has been in the past) by commercial competitors who view open-source technologies and decentralized networks as threats to their market power. Conversely, fediverse enthusiasts may introduce the threat of *technoromanticism* in overstating the role of technology in promoting democratic values or maximizing efficiency, or overstating the centrality of a single innovator in crafting a narrative around technological

innovation. This utopian discourse poses a threat to the fediverse because it distracts from the importance of collective social action in the development of technology. It also serves as a vector of neoliberal ideology, privileging the value of market-based interventions that subvert the core civic value of the fediverse's fundamentally noncommercial, decentralized building blocks.

Among the people leading adoption and design of the fediverse, many of these issues have already been identified and discussed. But the field has yet to coalesce in a conversation about how to manage governance and growth in a distributed, federated environment, with the aim of establishing a healthy, inclusive, and stable digital public sphere. We hope that this systematic overview of the potential threats to the fediverse, and our discussion about how to identify them and limit their impact, is a critical step toward reaching those civic and technosocial goals together.

References

Abad-Santos, A. (2015, July 8). *The Reddit revolt that led to CEO Ellen Pao's resignation, explained*. Vox. Retrieved from https://www.vox.com/2015/7/8/8914661/reddit-victoria-protest

Arkko, J., Trammell, B., Nottingham, M., Huitema, C., Thomson, M., Tantsura, J., & ten Oever, N. (2019, July 8). *Considerations on Internet consolidation and the Internet architecture*. Internet Engineering Task Force. Retrieved from https://datatracker.ietf.org/doc/draft-arkko-iab-internet-consolidation

Barber, G. (2023, July 18). Meta's Threads could make—or break—the Fediverse. *Wired*. Retrieved from https://www.wired.com/story/metas-threads-could-make-or-break-the-fediverse/

Black, M. L. (2022). *Transparent designs: Personal computing and the politics of user-friendliness*. Baltimore, MD: Johns Hopkins University Press.

Boutin, P. (2004, April 15). Read my mail, please. *Slate*. Retrieved from https://slate.com/technology/2004/04/the-silly-fears-about-google-s-e-mail-service.html

Butler, P. (2022, December 16). *What is Mastodon, the alternative social network now blocked by Twitter?* CNET. Retrieved from https://www.cnet.com/tech/services-and-software/what-is-mastodon-the-alternative-social-network-now-blocked-by-twitter/

Cabello, F., Franco, M. G., & Haché, A. (2013). Towards a free federated social Web: Lorea takes the networks! In G. Lovink & M. Rausch (Eds.), *Unlike us reader: Social media monopolies and their alternatives* (pp. 338–346). Amsterdam, The Netherlands: Institute of Network Cultures.

Caelin, D. (2022). Decentralized networks vs the trolls. In H. Mahmoudi, M. H. Allen, & K. Seaman (Eds.), *Fundamental challenges to global peace and security: The future of humanity* (pp. 143–168). Cham, Switzerland: Springer International Publishing. doi:10.1007/978-3-030-79072-1_8

Caplan, R., & Gillespie, T. (2020). Tiered governance and demonetization: The shifting terms of labor and compensation in the platform economy. *Social Media + Society, 6*(2), 1–13. doi:10.1177/2056305120936636

Carey, J. W., & Quirk, J. J. (1970). The mythos of the electronic revolution. *The American Scholar, 39*(3), 395–424.

Clark, M. (2021, October 29). *Mastodon puts Trump's social network on notice for improperly using its code*. The Verge. Retrieved from https://www.theverge.com/2021/10/29/22752850/mastodon-trump-truth-social-network-open-source-gab-legal-notice

Coeckelbergh, M. (2017). *New romantic cyborgs: Romanticism, information technology, and the end of the machine*. Cambridge, MA: MIT Press.

Coombs, W. T., & Holladay, S. J. (2006). Unpacking the halo effect: Reputation and crisis management. *Journal of Communication Management, 10*(2), 123–137. doi:10.1108/13632540610664698

Corbet, J. (2015, March 25). *Development activity in LibreOffice and OpenOffice*. LWN.Net. Retrieved from https://lwn.net/Articles/637735/

Corbett, F., & Spinello, E. (2020). Connectivism and leadership: Harnessing a learning theory for the digital age to redefine leadership in the twenty-first century. *Heliyon, 6*(1), 1–9. doi:10.1016/j.heliyon.2020.e03250

Coyne, R. (1999). *Technoromanticism: Digital narrative, holism, and the romance of the real*. Cambridge, MA: MIT Press.

DeNardis, L. (2020). *The Internet in everything: Freedom and security in a world with no off switch*. New Haven, CT: Yale University Press.

Dewey, J. (1927). *The public and Its problems*. New York, NY: Holt.

Doctorow, C. (2017, September 18). *An open letter to the W3C director, CEO, team and membership*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2017/09/open-letter-w3c-director-ceo-team-and-membership

Doctorow, C. (2019, May 29). *How DRM has permitted Google to have an "open source" browser that is still under its exclusive control*. Boing Boing. Retrieved from https://boingboing.net/2019/05/29/hoarding-software-freedom.html

Doctorow, C. (2023, January 21). Pluralistic: Tiktok's enshittification. *Pluralistic*. Retrieved from https://pluralistic.net/2023/01/21/potemkin-ai/

Driscoll, K. (2023, April 3). Do we misremember Eternal September? *Flow Journal*. Retrieved from https://www.flowjournal.org/2023/04/eternal-september/

Dunbar-Hester, C. (2024). Showing your ass on Mastodon: Lossy distribution, hashtag activism, and public scrutiny on federated, feral social media. *First Monday, 29*(3–4). doi:10.5210/fm.v29i3.13367

Field, H., & Vanian, J. (2023, June 16). *Reddit is in crisis as prominent moderators loudly protest the company's treatment of developers*. CNBC. Retrieved from https://www.cnbc.com/2023/06/16/reddit-in-crisis-as-prominent-moderators-protest-api-price-increase.html

Fischer, S. (2020, June 29). *Reddit bans The_Donald forum as part of major hate speech purge*. Axios. Retrieved from https://www.axios.com/2020/06/29/reddit-bans-the_donald-forum-as-part-of-major-hate-speech-purge

Fried, I. (2020, March 12). *Google's G Suite cracks 2 billion users*. Axios. Retrieved from https://www.axios.com/2020/03/12/google-g-suite-total-users

Gehl, R. W. (2016). Power/freedom on the dark Web: A digital ethnography of the dark Web social network. *New Media & Society, 18*(7), 1219–1235. doi:10.1177/1461444814554900

Gehl, R. W., & Zulli, D. (2023). The digital covenant: Non-centralized platform governance on the mastodon social network. *Information, Communication & Society, 26*(16), 3275–3291. doi:10.1080/1369118X.2022.2147400

Giblin, R., & Doctorow, C. (2022). *Chokepoint capitalism: How big tech and big content captured creative labor markets and how we'll win them back*. Boston, MA: Beacon Press.

Gibson, A. D. (2023). What teams do: Exploring volunteer content moderation team labor on Facebook. *Social Media + Society, 9*(3), 1–10. doi:10.1177/20563051231186109

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. New Haven, CT: Yale University Press.

Gillespie, T., Aufderheide, P., Carmi, E., Gerrard, Y., Gorwa, R., Matamoros-Fernández, A., . . . West, S. M. (2020). Expanding the debate about content moderation: Scholarly research agendas for the coming policy debates. *Internet Policy Review, 9*(4), 1–30. doi:10.14763/2020.4.1512

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society, 22*(6), 854–871. doi:10.1080/1369118X.2019.1573914

Gorwa, R., & Ash, T. G. (2020). Democratic transparency in the platform society. In J. A. Tucker & N. Persily (Eds.), *Social media and democracy: The state of the field, prospects for reform* (pp. 286–312). Cambridge, UK: Cambridge University Press.

Gow, G. (2022). *Turning to alternative social media*. In L. Sloan & A. Quan-Haase (Eds.), *The SAGE handbook of social media research methods* (pp. 568–580). London, UK: SAGE. doi:10.4135/9781529782943

Grimmelmann, J. (2015). *The virtues of moderation*. Yale Journal of Law and Technology. Retrieved from https://openyls.law.yale.edu/handle/20.500.13051/7798

Gülcü, C. (2001). *Log4j* [Computer software]. Wakefield, MA: Apache Software Foundation.

Halfaker, A., Geiger, R. S., Morgan, J. T., & Riedl, J. (2013). The rise and decline of an open collaboration system: How Wikipedia's reaction to popularity is causing its decline. *American Behavioral Scientist, 57*(5), 664–688. doi:10.1177/0002764212469365

Hall, S., Critcher, C., Jefferson, T., Clarke, J., & Roberts, B. (1978). *Policing the crisis: Mugging, the state and law and order*. London, UK: Macmillan.

Hawkins, S. (2005). Beyond the digital divide: Issues of access and economics. *Canadian Journal of Information & Library Sciences, 29*(2), 171–189.

Heath, A. (2023, June 8). *This is what Instagram's upcoming Twitter competitor looks like*. The Verge. Retrieved from https://www.theverge.com/2023/6/8/23754304/instagram-meta-twitter-competitor-threads-activitypub

Hendrix, J., & Flowers, J. (2022, November 23). *The whiteness of Mastodon*. Tech Policy Press. Retrieved from https://techpolicy.press/the-whiteness-of-mastodon/

Hill, B. M. (2018, June 19). *How markets coopted free software's most powerful weapon* (LibrePlanet '18 keynote) [Video file]. YouTube. Retrieved from https://www.youtube.com/watch?v=vBknF2yUZZ8

Hoffmann, A. L., Proferes, N., & Zimmer, M. (2018). "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society, 20*(1), 199–218. doi:10.1177/1461444816660784

John, N. A. (2019). Social media bullshit: What we don't know about facebook.com/peace and why we should care. *Social Media + Society, 5*(1), 1–16. doi:10.1177/2056305119829863

Jones, C. (2024, February 2). *Critical vulnerability in Mastodon sparks patching frenzy*. The Register. Retrieved from https://www.theregister.com/2024/02/02/critical_vulnerability_in_mastodon_is/

Lemmer-Webber, C., Tallon, J., Shephard, E., Guy, A., & Prodromou, E. (2018, January 23). *ActivityPub*. World Wide Web Consortium (W3C). Retrieved from https://www.w3.org/TR/activitypub/

Li, H., Hecht, B., & Chancellor, S. (2022). Measuring the monetary value of online volunteer work. *Proceedings of the International AAAI Conference on Web and Social Media, 16*, 596–606. doi:10.1609/icwsm.v16i1.19318

Mac, R., & Hsu, T. (2023, July 24). From Twitter to X: Elon Musk begins erasing an iconic Internet brand. *The New York Times*. Retrieved from https://www.nytimes.com/2023/07/24/technology/twitter-x-elon-musk.html

Makuch, B. (2019, July 11). The Nazi-free alternative to Twitter is now home to the biggest far right social network. *Vice*. Retrieved from https://www.vice.com/en/article/mb8y3x/the-nazi-free-alternative-to-twitter-is-now-home-to-the-biggest-far-right-social-network

Mansoux, A., & Roscam Abbing, R. (2020). Seven theses on the fediverse and the becoming of floss. In K. Gansing & I. Luchs (Eds.), *The eternal network* (pp. 124–140). Amsterdam, The Netherlands: Institute of Network Cultures.

Marshall, J. (2006). Negri, Hardt, distributed governance and open source software. *PORTAL Journal of Multidisciplinary International Studies, 3*(1), 1–25. doi:10.5130/portal.v3i1.122

Matias, J. N. (2016). Going dark: Social factors in collective action against platform operators in the Reddit blackout. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 1138–1151). New York, NY: Association for Computing Machinery. doi:10.1145/2858036.2858391

Mehta, I. (2023, March 9). *Meta is working on a decentralized social app*. TechCrunch. Retrieved from https://techcrunch.com/2023/03/09/meta-is-working-on-a-decentralized-social-app/

Mejias, U. A. (2012). Liberation technology and the Arab Spring: From utopia to atopia and beyond. *The Fibreculture Journal, 20*, 204–217.

Mueller, M., & Farhat, K. (2023, March 1). *TikTok and U.S. national security*. Internet Governance Project. Retrieved from https://www.internetgovernance.org/research/tiktok-and-us-national-security/

Music & Copyright. (2023, April 25). *Music & copyright*. Retrieved from https://musicandcopyright.wordpress.com/2023/04/25/recorded-music-market-share-gains-for-sme-and-the-indies-publishing-share-growth-for-umpg-and-wcm/

Napoli, P., & Caplan, R. (2017). Why media companies insist they're not media companies, why they're wrong, and why it matters. *First Monday,* 22(5). doi:10.5210/fm.v22i5.7051

Opsahl, K. (2021, August 11). *If you build it, they will come: Apple has opened the backdoor to increased surveillance and censorship around the world*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2021/08/if-you-build-it-they-will-come-apple-has-opened-backdoor-increased-surveillance

Paul, R. (2010a, September 28). *Document Foundation forks OpenOffice.org, liberates it from Oracle*. Ars Technica. Retrieved from https://arstechnica.com/information-technology/2010/09/document-foundation-forks-openofficeorg-to-liberate-it-from-oracle/

Paul, R. (2010b, October 18). *Oracle wants LibreOffice members to leave OOo council*. Ars Technica. Retrieved from https://arstechnica.com/information-technology/2010/10/oracle-wants-libreoffice-members-to-leave-ooo-council/

Phillips, W., & Milner, R. M. (2021). *You are here: A field guide for navigating polarized speech, conspiracy theories, and our polluted media landscape*. Cambridge, MA: The MIT Press. doi:10.7551/mitpress/12436.001.0001

Reddit. (2012, February 12). *A necessary change in policy*. Reddit. Retrieved from www.reddit.com/r/blog/comments/pmj7f/a_necessary_change_in_policy/

Roberts, S. T. (2019). *Behind the screen: Content moderation in the shadows of social media*. New Haven, CT: Yale University Press.

Rochko, E. (2023, May 1). *A new onboarding experience on Mastodon*. Mastodon Blog. Retrieved from https://blog.joinmastodon.org/2023/05/a-new-onboarding-experience-on-mastodon/

Roscam Abbing, R., Diehm, C., & Warreth, S. (2023). Decentralised social media. *Internet Policy Review, 12*(1), 1–11. doi:10.14763/2023.1.1681

Sevignani, S. (2013). Facebook vs. diaspora: A critical study. In G. Lovink & M. Rausch (Eds.), *Unlike us reader: Social media monopolies and their alternatives* (pp. 323–337). Amsterdam, The Netherlands: Institute of Network Cultures.

Sinnreich, A. (2013). *The piracy crusade: How the music industry's war on sharing destroys markets and erodes civil liberties*. Amherst: University of Massachusetts Press.

Sinnreich, A., Aufderheide, P., Clifford, M., & Shahin, S. (2021). Access shrugged: The decline of the copyleft and the rise of utilitarian openness. *New Media & Society, 23*(12), 3466–3490. doi:10.1177/1461444820957304

Sinnreich, A., & Gilbert, J. (2024). *The secret life of data: Navigating hype and uncertainty in the age of algorithmic surveillance*. Cambridge, MA: The MIT Press.

Smith, E. (2022, November 14). *The infernal September*. Tedium: The Dull Side of the Internet. Retrieved from https://midrange.tedium.co/issues/mastodon-eternal-september-discussion/

Smith, E. (2023, May 31). *Ernie Smith* (@ernie@writing.exchange). Writing Exchange. Retrieved from https://writing.exchange/@ernie/110463600042130703

Srnicek, N. (2017). *Platform capitalism*. Cambridge, UK: Polity.

Starks, T. (2021, December 13). *CISA warns "most serious" Log4j vulnerability likely to affect hundreds of millions of devices*. CyberScoop. Retrieved from https://cyberscoop.com/log4j-cisa-easterly-most-serious/

Streeter, T. (1987). The cable fable revisited: Discourse, policy, and the making of cable television. *Critical Studies in Mass Communication, 4*(2), 174–200. doi:10.1080/15295038709360124

Streeter, T. (2010). *The net effect: Romanticism, capitalism, and the Internet*. New York: New York University Press. doi:10.18574/9780814708743

Suderman, A. (2022, July 14). *Log4j software flaw "endemic," new cyber safety panel says*. AP News. Retrieved from https://apnews.com/article/biden-technology-software-hacking-4361f6e9b386259609b05b389db4d7bf

Thiel, D., & DiResta, R. (2023). *Child safety on federated social media.* Stanford Digital Repository. Retrieved from https://purl.stanford.edu/vb515nd6874

Turton, W., Gillum, J., & Robertson, J. (2021, December 13). *Inside the race to fix a potentially disastrous software flaw*. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2021-12-13/how-apache-raced-to-fix-a-potentially-disastrous-software-flaw

Vogels, E. A., Gelles-Watnick, R., & Massart, N. (2022, August 10). *Teens, social media and technology 2022*. Pew Research Center: Internet, Science & Tech. Retrieved from https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

Walker, L. (2004, April 15). AOL's garden might flourish without Rainman. *Washington Post*. Retrieved from https://www.washingtonpost.com/archive/business/2004/04/15/aols-garden-might-flourish-without-rainman/cdf8f533-7705-47c1-99af-65797692ae2c/

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society, 58*(1), 20–41. doi:10.1177/0007650317718185

Wiggers, K. (2023, April 18). Reddit will begin charging for access to its API. *TechCrunch*. Retrieved from https://techcrunch.com/2023/04/18/reddit-will-begin-charging-for-access-to-its-api/

Wu, T. (2010). *The master switch: The rise and fall of information empires* (1st ed.). New York, NY: Alfred A. Knopf.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum, 28*(1), 10–29. doi:10.1177/1095796018819461

Zulli, D., Liu, M., & Gehl, R. (2020). Rethinking the "social" in "social media": Insights into topology, abstraction, and scale on the Mastodon social network. *New Media & Society, 22*(7), 1188–1205. doi:10.1177/1461444820912533