

What rules are we following in Decentralized Networks? Privacy Policies, Instance rules and descriptions in Mastodon

Shrushti Kaul¹, Mehmet S. Aktas², Mirela Riveni¹

¹University of Groningen

²Yildiz Technical University

s.u.kaul@student.rug.nl, aktas@yildiz.edu.tr, m.riveni@rug.nl

Abstract

Alternative, Decentralized Social Networks are gaining much attention as the preferred online public spaces for users who are concerned about privacy and respectful environments. Investigating the rules by which the communication in these systems is guided is crucial, as privacy issues, freedom of speech, and regulations are pressing questions. This work presents our investigation on privacy policies, server rules and extended descriptions on Mastodon instances. Our results show that a number of instances on Mastodon follow the policies described on mastodon.social.

1 Introduction

In recent times, larger and more traditional social networking platforms have come under intense scrutiny because of their centralized control, with the power to shape the user experience and exploit users' data for profit, which in the past was done even without obtaining the consent of the individuals affected (Rochko 2018; 201 2016). This centralization has raised concerns about privacy, data ownership and control, leading to a rise in interest for alternative social media models. The Fediverse¹ is an alternative approach to social networking that emphasizes decentralization, interoperability, and trust. Unlike the conventional, centralized networks, the Fediverse is a collective of various social media services. These services are developed collaboratively by a global community of developers and users who are motivated by a desire to escape the restrictive and sometimes ethically questionable practices of monolithic corporate platforms. Traditional social networking sites own and monetize personal information. In stark contrast, the decentralized architecture of Fediverse ensures that no single entity has ownership of user data [3]. This structural and operational difference empowers individuals to choose with whom they share their information, thereby offering them enhanced control over their online interactions and privacy. One of the standout platforms within the Fediverse is Mastodon², a microblogging service that positions itself as a privacy-centric alternative to Twitter. Mastodon prioritizes user privacy from the

ground up. It operates through various independent servers called instances, each managed by an administrator responsible for maintaining the instances's integrity.³ This decentralized management model allows users to have significant control over their digital footprint, including who can view their posts and the ability to delete their content at their discretion (Budington 2022). The underlying motivation for this research is to investigate and understand the prevailing trends in how Mastodon servers describe themselves. This understanding is achieved by systematically extracting and analyzing the privacy policies, server rules, and extended descriptions of numerous Mastodon servers. The main research question we tackle in this work is to identify the recurring themes or topics that the instances emphasize, shedding light on the broader values and concerns that shape the Mastodon community and the Fediverse at large. Our findings show that many instances take an example of the privacy policy defined in mastodon.social, which is the server hosted by the founder of Mastodon, and that server descriptions and rules incorporate behavioral rules of respect, tolerance, non-discrimination and ethical social values.

This paper is structured as follows: the introduction is followed by a discussion on related work in Section 2. Section 3 follows with an outline of the pipeline applied for the analysis, which includes creating the corpora for privacy policies, extended descriptions and server rules and technologies used to extract prominent keywords/themes. Section 4 gives insight on the results retrieved after performing our analysis on the policies, descriptions and rules. In Section 5 we conclude the study and discuss a direction towards the prospective future work based on this initial exploration.

2 Related Work

Research on decentralised networks as ethical, privacy-preserving substitutes for conventional, centralized systems has been increasing in recent years. We can characterize these works in three main groups of research: a) technical frameworks and architectures for decentralization, b) governance, and moderation in distributed social networks, and c) user behavior and community norms.

2.1 Frameworks and Architectures

The first set of research papers examines system topologies and policy enforcement in decentralized systems. Wang and Minsky suggested a regularity-based decentralized social network architecture, combining the benefits of decentralization with scalable methods for describing and enforcing global social regularities (Wang and Minsky 2015). Presenting a decentralized social network architecture based on blockchain, Sarathchandra and Jayawikrama attempt to solve privacy concerns and improve control over information and interactions (Sarathchandra and Jayawikrama 2021). Thakur and Breslin underline the need of content governance in decentralized contracts (Thakur and Breslin 2021). Badis et al. have developed an asynchronous model for profile updates to improve data synchronization in federated networks (Bais et al. 2017). In contrast to these system-centered forms of analysis, our study focuses on the interpretive layer of instance-level metadata, examining how ideals about decentralization and governance are articulated through text in server descriptions, rules, and policies.

2.2 Administrative concerns and moderation

The second study category focuses on distributed social networks administrative concerns and moderation. For example, Anaobi et al. investigated pressures placed on managers of Mastodon, and subsequently presented a semi-automated moderation tool (Anaobi et al. 2023). This contributes to the conversation about the challenges that federated spaces face concerning the maintenance of freedoms away from enforcement. Another study by (Bono et al. 2024) sheds light on moderation performed by servers by *blocklisting* other servers with problematic content, showcasing a pattern of a “cluster” of banned instances. Another moderation tool is introduced by (Riemann 2022), namely the Mastodon Privacy Policy Generator, that helps Mastodon admins in creating privacy policies that are GDPR and CCPA compliant. Additionally, work in (Rozenstein 2022) highlights how moderation can vary across instances, often driven by regional motivations or norms which only adds to the complexity of moderation. For instance, *mastodon.social* is hosted in Germany, and thus bans content that is illegal there and *Twitter* – permitted advertisements that would otherwise be mostly prohibited on different instances (Rozenstein 2022). Although these investigations and tools underscore enforcement and administrative challenges, our effort attends to the normative messaging that is encoded in server guidelines themselves, and demonstrate how values of community governance can be articulated at scale.

2.3 User engagement

The third category addresses user engagement, profiling, and trends that emerged across distributed social networks. Hironaka et al. compared the usage of Mastodon with Twitter, and specifications were limited to discourses that were community-based that existed on Mastodon (Hironaka et al. 2024). Al-Khateeb provided scripts and exploratory method(s) to detect trending topics on Mastodon (Al-Khateeb 2022). Bertino et al. examined user deception and

Category	With Content	With English Content
Privacy Policies	9445	8325
Server Rules	6244	4052
Extended Descriptions	6116	4025

Table 1: Statistics on the availability of different types of content on Mastodon servers. All values are out of a total of 18,866 instances.

privacy strategies with a psychological perspective on how users manage identity in social systems (Bertino, Caverlee, and Ferrari 2014). Our research shifts focus away from user-focused behaviour or personality analyses to emphasize the institutional voice of Mastodon instances, particularly studying the written forms of server-level social contracts that include values such as inclusivity and trust.

Overall, in contrast to the aforementioned previous studies, this research shifts from research based on infrastructure development, to focus on the explicit textual artifacts within communities that regulate behavior within a distributed social network such as Mastodon: privacy policies, server rules and guidelines, and extended server descriptions. This paper, adds value to the existing performance perspective works, with that we examine how values such as inclusivity, non-discrimination, and trust appear in metadata associated with servers. This work aligns with efforts of the likes of (Nicholson, Keegan, and Fiesler 2023) that characterize formal rules across Mastodon servers into various themes and compare them to Reddit’s subreddit-based rules structures. Our work complements Nicholson et al.’s approach by analyzing an even higher number of artifacts. We argue that this meta-level examination is an important aspect that helps lend a unique persona into the culture that has shaped the Fediverse from the ground up and brings together technical architecture with community values.

3 Methodology

3.1 Dataset

We first retrieved the list of up and running Mastodon instances. This was achieved using the *instance.social* API⁴, which is a website that is used to find an appropriate Mastodon instance to join. We retrieved a list of a total of 18866 Mastodon servers.

We retrieve three key pieces of information per instance from this server list, as in the following;

- Privacy policy. It is scraped from the website with the help of Selenium WebDriver.
- Extended description. This is the “About” section displayed in the Mastodon home page, but within the Mastodon API⁵, it’s called as “Extended Description”. As aforementioned, there is an API to extract the content for this section and this content is in free-form string.
- Server rules. The Mastodon API⁵ allows us to retrieve the rules as a JSON array with each element consisting of one rule. Each rule on itself is a free-form string.

⁴<https://instances.social/>

⁵<https://docs.joinmastodon.org/client/intro/>

the said terms based on instance types, classified by country, dedicated topics of discussion, and the size of instances.

References

2016. Distributed Social Networks and Public History, <https://publichistory.media/2016/02/21/distributed-social-networks-and-public-history/>.
- Al-Khateeb, S. 2022. Dapping into the Fediverse: Analyzing What's Trending on Mastodon Social. In *Social, Cultural, and Behavioral Modeling*, volume 13558 of *Lecture Notes in Computer Science*. Springer, Cham.
- Anaobi, I. H.; Raman, A.; Castro, I.; Bin Zia, H.; Ibosiola, D.; and Tyson, G. 2023. Will Admins Cope? Decentralized Moderation in the Fediverse. In *Proceedings of the ACM Web Conference 2023*, 3109–3120.
- Bais, L.; et al. 2017. Asynchronous model for updating replicated profiles in decentralized social network. In *2017 International Conference on Mathematics and Information Technology (ICMIT)*. IEEE.
- Bertino, E.; Caverlee, J.; and Ferrari, E. 2014. Identity, privacy, and deception in social networks. *IEEE Internet Computing*, 18(2): 7–9.
- Blei, D. M.; Ng, A. Y.; and Jordan, M. I. 2003. Latent dirichlet allocation. *J. Mach. Learn. Res.*, 3(null): 993–1022.
- Bono, C. A.; La Cava, L.; Luceri, L.; and Pierri, F. 2024. An Exploration of Decentralized Moderation on Mastodon. In *Proceedings of the 16th ACM Web Science Conference, WEBSCI '24*, 53–58. New York, NY, USA: Association for Computing Machinery. ISBN 9798400703348.
- Budington, B. 2022. Is Mastodon Private and Secure? Let's Take a Look, <https://www.eff.org/deeplinks/2022/11/mastodon-private-and-secure-lets-take-look>.
- Hironaka, S.; et al. 2024. Comparing User Activity on X and Mastodon. *2024 IEEE International Conference on Big Data (BigData)*.
- Hwang, S.; Nanayakkara, P.; and Shvartzshnaider, Y. 2023. Whose Policy? Privacy Challenges of Decentralized Platforms. In *CHI '23 Workshops: Designing Technology and Policy Simultaneously: Towards A Research Agenda and New Practice*. <https://ssrn.com/abstract=4416746> or <https://www.sohyeonhwang.com/docs/CHI2023.Workshop.DesignPolicy.pdf>.
- Nicholson, M. N.; Keegan, B. C.; and Fiesler, C. 2023. Mastodon Rules: Characterizing Formal Rules on Popular Mastodon Instances. In *Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing, CSCW '23 Companion*, 86–90. New York, NY, USA: Association for Computing Machinery. ISBN 9798400701290.
- Riemann, R. 2022. Mastodon Privacy Policy Generator. Helps Mastodon admins adapt privacy policies for GDPR compliance. Version v1.1 released on November 22, 2022.
- Rochko, E. 2018. #DeleteFacebook, <https://blog.joinmastodon.org/2018/03/delete-facebook/>.
- Rozenstein, O. 2022. Moderating the Fediverse: Content Moderation on Distributed Social Media. Date Written: November 23, 2022; Last revised: June 5, 2023.
- Sarathchandra, T.; and Jayawikrama, D. 2021. A decentralized social network architecture. In *2021 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, 251–257. IEEE.
- Thakur, S.; and Breslin, J. G. 2021. Rumour prevention in social networks with layer 2 blockchains. *Social Network Analysis and Mining*, 11(1): 104.
- Viégas, F. B.; and Wattenberg, M. 2008. Tag Clouds and the Case for Vernacular Visualization. *Interactions*, 15(4): 49–52.
- Wang, Z.; and Minsky, N. H. 2015. Regularity Based Decentralized Social Networks. (*CRiSIS 2014*).