NLUJ Law Review

Nikhil Mahadeva & Sharath Chandupatla, *Regulation of the Fediverse: The Multiverse of Social Media*, 9(1) NLUJ L. REV. 1 (2022).

REGULATION OF THE FEDIVERSE: THE MULTIVERSE OF SOCIAL MEDIA

~Nikhil Mahadeva & Sharath Chandupatla[*]

ABSTRACT

The Government of India has been persistent in its efforts to regulate big tech companies. In February 2021, it issued regulations imposing various obligations on social media, the use of which is of particular concern to the government, for a multitude of reasons. However, social media is constantly evolving. Mark Zuckerberg recently explained his vision for the future of social media with the change of Facebook's name to Meta -- a virtual reality 'metaverse'. While this metaverse is little more than a concept currently, there already exists something with a similar moniker - the 'Fediverse,' formed from a collection of Federated Social Networks, an overlooked type of social media that gives its users the right to exercise choice and protect their privacy by decentralising social media. The recent push by the European Union for interoperability and community-led platforms, both core features of Federated Social Networks, makes the Fediverse an important topic of discussion, as a possible representation of the future of social media. This is especially true given how its unique features present several

[*] Nikhil Mahadeva is currently a J.D. candidate at Columbia Law School, New York. He has a B.A. LL.B. (Hons.) from NUALS, Kochi and practiced in litigation, arbitration, and tech law prior to his J.D. He can be reached at nikhil.m@columbia.edu.
Sharath Chandupatla is a practicing Advocate before the Telangana High Court, focusing on tech law and data protection. He has a B.A. LL.B. (Hons.) from NUALS, Kochi. He can be reached at chandupatlasharath@gmail.com

difficulties in relation to its regulation. This paper intends to analyse the applicability of the current laws to this overlooked type of social media. First, it explains what a federated social network is and how it works. Second, it explains the laws which could conceivably be applied to them and the difficulty in enforcing those laws. On a concluding note, it moots the question of whether federated social networks should be regulated at all and if so, how?

TABLE OF CONTENTS

I. INTRODUCTION

India has recently enacted new rules for the regulation of intermediaries, with a specific focus on 'Social Media Intermediaries' ("**SMIs**") (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules**" or "**the Rules**"). The Rules were enacted in the wake of a disagreement between the Government of India and Twitter over a denial to take down tweets from its platform.[1] The move is part of a greater strategy to regulate speech on typical social media platforms, by putting their protected intermediary status at risk in cases of non-compliance.[2]

The prevailing presumption is that the Government has defined 'social media intermediaries' widely enough to have the ability to enforce these regulations in their current form on all kinds of social media platforms[3], and even possibly other services unrelated to social media.[4] Through this article, we seek to prove that this presumption is flawed when placed in the greater context of the different forms social media is taking, in contrast to what social media is popularly known to be.

Prima facie, States find it difficult to regulate and control the internet; it transcends control by any individual State because it does not represent a singular, definable entity but a larger collective outside of the reach of

---

[1] Soutik Biswas, *The Indian Government's war with Twitter,* BBC (Feb. 12, 2021), https://www.bbc.com/news/world-asia-india-56007451.

[2] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139, (India) Rule 7 (*hereinafter* "**IT Rules**").

[3] Shrey Fatterperkar, *IT Rules 2021 explained: Non-compliance will expose WhatsApp, Facebook, Twitter to significant liability,* FIRST POST May 27, 2021), https://www.firstpost.com/india/it-rules-2021-explained-non-compliance-will-expose-whatsapp-facebook-twitter-to-significant-liability-9661461.html.

[4] *X v. Union of India*, 2021 SCC OnLine Del 1788 (India).

unitary control. This sort of unitary control and regulation is, however, exercised by conventional social media (like Facebook and Twitter). These platforms, through their Terms of Service and Community Standards,[5] let users use them in a certain permitted manner while retaining control in the hands of the singular provider. Users are simply renters of a platform - they do not personally exercise any control. These platforms have 'centralized' control. This 'centralization' feels especially stark in the current paradigm, where a private individual like Elon Musk unilaterally owns and controls a massive conventional social media network like Twitter.[6]

It is immensely important to consider what the future of social media looks like at this juncture, as Governments across the globe are discussing how to mitigate the power conventional social media exercises. The typical manifestation of this is in antitrust actions, such as the case arguing for the breaking up of Meta.[7] However, another method that is seeing growing support is 'adversarial interoperability'.[8] Adversarial Interoperability is where a platform does not explicitly want third parties to be able to connect to or work with them, whether for reasons of revenue or maintaining a 'walled garden', but third parties are still able to do so.[9]

---

[5] Terms of Service, *Facebook*, https://www.facebook.com/terms.php; Twitter Terms of Service, *Twitter,* https://twitter.com/en/tos; Snap Inc. Terms of Service, *Snap Inc,* https://snap.com/en-US/terms.

[6] Sheila Dang & Greg Roumeliotis, *Musk begins his Twitter ownership with firings, declares the 'bird is freed',* REUTERS, (Oct. 28, 2022), https://www.reuters.com/markets/deals/elon-musk-completes-44-bln-acquisition-twitter-2022-10-28/.

[7] Rebecca Heilweil, *Why the US government wants Facebook to sell off Instagram and WhatsApp,* VOX (Dec. 09, 2020), https://www.vox.com/recode/221664.

[8] Cory Doctorow, *Adversarial Interoperability*, ELECTRONIC FRONTIER FOUNDATION, (Oct. 02, 2019), https://www.eff.org/deeplinks/2019/10/adversarial-interoperability.

[9] Shawn Wang, *Notes on Adversarial Interoperability,* SWYX (Sep. 13, 2020), https://www.swyx.io/adversarial_interoperability.

Adversarial interoperability is the reason cars can be fixed with parts made by someone other than the original manufacturer, or third party ink can be used in a printer. Crucially, it can be forced by lawmakers by enacting laws. For example, legislators can mandate Facebook to allow a Twitter user to post on Facebook, or vice versa. In fact, in its most recent move to regulate big tech companies, the European Union has passed the Digital Markets Act, a part of which mandates interoperability between messaging platforms such as WhatsApp, iMessage, Telegram, etc.[10] In the same vein, experts on social media regulation strongly recommend a shift of focus, from building platforms to building protocols.[11]

To add to this, the European Parliament also commissioned the Greens/EFA group to submit a report on community led platforms, in comparison to conventional social media platforms.[12] The study report made several recommendations in relation to content moderation on social media platforms, suggesting that they democratise platforms' terms of services, have community led content moderation and support community led platforms which will help in building a healthy social media space, in comparison to the authoritative style of content moderation employed by conventional social media platforms.

---

[10] Morgan Meaker, *Europe's Digital Market Act takes Hammer to Big Tech*, WIRED (Mar. 25, 2022), https://www.wired.co.uk/article/digital-markets-act-messaging.

[11] Mike Masnick, *Protocols Not Platforms: A Technological Approach to Free Speech,* KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY (Aug. 21, 2019), https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech.

[12] BEN WAGNER ET AL., REIMAGINING CONTENT MODERATION AND SAFEGUARDING FUNDAMENTAL RIGHTS A STUDY ON COMMUNITY-LED PLATFORMS, The Greens/EFA (2021).

This is where decentralised social media comes in. While conventional social media platforms centralise power with the company which created them, decentralised social media, also known as 'Federated Social Networks' ("**FSN**"), do the exact opposite.[13] They give power to individual users and exercise minimal power themselves.[14] They represent a manifestation of everything mentioned above - they are interoperable by design, community led, and built on protocols that are open source and platform agnostic. Knowingly or unknowingly, the measures and discussions mentioned above all lead to making conventional social media more like FSNs. However, these platforms already exist, and are growing in popularity. The acquisition of Twitter by Elon Musk, for example, has led to a mass exodus of users from Twitter to Mastodon, giving Mastodon an additional 2 million monthly active users since the acquisition was finalized.[15] Whether it is in their existing form, or when conventional social media is eventually forced to take on all of their requisite features, we argue that they represent the future of social media: private, flexible and user-centric.[16]

Currently, no country in the world specifically regulates or has legislated on FSNs. The discussion on whether they need to be regulated

---

[13] Adi Robertson, *How the Biggest Decentralized Social Network is dealing with its Nazi Problem,* THE VERGE (Jul. 12, 2019), https://www.theverge.com/2019/7/12/20691957/mastodon-decentralized-social-network-gab-migration-fediverse-app-blocking.

[14] Richard Esguerra, *An Introduction to the Federated Social Network,* EFF.ORG (Mar. 21, 2011), https://www.eff.org/deeplinks/2011/03/introduction-distributed-social-network.

[15] Jay Peters, *More than two million users have flocked to Mastodon since Elon Musk took over Twitter*, THE VERGE (Dec. 20, 2022), https://www.theverge.com/2022/12/20/23518325/mastodon-monthly-active-users-twitter-elon-musk.

[16] Tulane University, *What You Need to Know About Decentralized Social Networks,* SOPA - TULANE UNIVERSITY (Dec. 20, 2022, 12:01 PM), https://sopa.tulane.edu/blog/decentralized-social-networks.

or not, and how that may be achieved, is sparse (with the exception of the above-mentioned report) despite their growing popularity. The intention of this article is to raise the question of how FSNs are treated under the law currently, and how they ought to be in the future. The rapid development and virality of technology regularly out-paces legal regulation. Thus, it is imperative that we address the issues a new technology may present sooner rather than later, so action can be more expedient when it inevitably becomes necessary. The lessons learned from the failure to regulate conventional social media until recently serve to underscore this point.[17] If the nature of social media is inevitably to change, then FSNs may prove to be the natural next step in that evolution, whose regulation needs to be discussed now given the user privacy and data autonomy they offer to users.

As of now, the Indian Government's only response to the discussion on regulating any kind of social media is the IT Rules. Through the IT Rules, the Government intends to seize power over speech from conventional social media.[18] Experts opine that *"[t]hese Rules are another tool in the hands of the government to use law enforcement agencies and other means to go after individuals who express opinions which run contrary to its ideas and interests*".[19] Yet, the existence of FSNs raises the question of how a government can

[17] Andrew Arnold, *Do We Really Need To Start Regulating Social Media?,* FORBES (Jul. 30, 2018) https://www.forbes.com/sites/andrewarnold/2018/07/30/do-we-really-need-to-start-regulating-social-media/?sh=69cac1a2193d; Michael A. Cusumano, Annabelle Gawer, and David B. Yoffie, *Social Media Companies Should Self-Regulate. Now.,* HARVARD BUSINESS REVIEW (Jan. 15, 2021), https://hbr.org/2021/01/social-media-companies-should-self-regulate-now.

[18] Raghav Tankha, *The Information Technology Rules 2021: An assault on Privacy as we know it,* BAR AND BENCH (Mar 09, 2021) https://www.barandbench.com/columns/the-information-technology-rules-2021-an-assault-on-privacy-as-we-know-it.

[19] *Id.*

take power away from an entity that does not have any effective regulatory powers in the first place, and how enforcement under the new IT Rules is going to impact these platforms.

This article will attempt to address these concerns. *First*, we explain what an FSN is, and how it works; Second, we examine whether an FSN falls under the definition of an intermediary and/or an SMI under the existing law; Third, we discuss how these laws may become applicable to such platforms and the issues that would arise from attempting to enforce them; Finally, we moot whether FSNs should be regulated at all, and if so, how?

A. NATURE AND FUNCTIONING OF FSNS

FSNs are functionally similar to conventional social media networks; most permit you to share statuses, message friends, and upload content, among other things. Mastodon is a good example of an FSN - it is built to be parallel to Twitter. There is a feed, on which one can see 'toots' (the Mastodon equivalent of tweets), which can be 'boosted' (retweeted), or 'favourited' (liked). Similarly, messages can also be sent. Overall, the interface is quite similar.[20]

However, being an FSN, Mastodon has a significantly different structure than Twitter. On Twitter, all activity is carried out on Twitter's servers, and all information remains stored on those servers.[21] On an FSN, users do not all go through a single server or a single provider to use these

[20] Mastodon, *What is Mastodon?*, YOUTUBE (Mar. 23, 2018), https://youtu.be/IPSbNdBmWKE.

[21] Twitter, *How to Access your Twitter Data*, (last visited Oct. 18, 2021) https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data.

features.[22] Instead, the provider here, like Mastodon, gives an individual access to their software. This software is open source, and an individual can use it to host information on their own server or choose to register with a server hosted by someone else. In the example of Mastodon, these servers are called 'instances.'[23]

These 'instances' can then, through the software, communicate with any other server running the same or similar technology.[24] The key here however, is that the FSN has no control over any of the user's information - they simply provide a software framework for these functions to happen and for these instances to be connected.[25] The actual information is stored not by the FSN, but by the user on their own private instance, or on an instance they choose to register with, hosted by someone else. Though FSNs are technically 'public' in nature, these instances are usually tight-knit communities with limited intake; this can depend on factors like capacity or a unifying characteristic like a specific interest. These communities are governed by themselves or the persons who host them - not by the FSN itself.

While a user's information is on a single instance, they can still communicate with the potentially infinite other instances on the greater

---

[22] Esseguara, *supra* note 14.
[23] Divya Kala Bhavani and Naresh Singaravelu, *What is Mastodon, the new social media kid on the block,* THE HINDU (Nov. 08, 2019), https://www.thehindu.com/sci-tech/technology/internet/what-is-mastodon-the-new-social-media-kid-on-the-block/article29924482.ece.
[24] *Id.*
[25] David Thomas, *Distributed Social Networks and Federation: Why They're Important For Privacy and Online Safety,* SABAI TECHNOLOGY (Oct. 9, 2020), https://www.sabaitechnology.com/blog/distributed-social-networks-and-federation-why-theyre-important-for-privacy-and-online-safety/.

'network' of instances operated by others. This means a user's information is in their control, but they can still connect with other people as they would normally on a social media network.[26] They can post a message across instances, or choose to make it as private as possible, and the distinction would be far more meaningful as it is not just the viewability of the information being changed, but the dissemination of it across actual servers.[27] This is of course not discounting the ability to freely communicate within a user's own instance, should it be one with other people.

While we have used Mastodon as an example, it is only one of many FSNs. Just as with conventional social media, there are many other FSNs with different features. Another example is PixelFed,[28] made by the same developers behind Mastodon. PixelFed is an Instagram alternative focused on image sharing. Similarly, there are Diaspora,[29] Friendica,[30] Peertube[31] (an alternative to YouTube), Plume,[32] and a multitude of others.

The presence of so many alternatives lead us to another central function of FSNs: the connection between services. Not only can instances communicate within the network of the software they are using, but also, to some extent, with servers running other FSN software.[33] This is achieved by using common communication protocols across software – meaning a person using Mastodon could communicate with another person using

---

[26] Esseguara, *supra* note 14.
[27] *Id.*
[28] PixelFed, https://pixelfed.org/ (last visited Oct. 19, 2021).
[29] JoinDiaspora, https://joindiaspora.com/ (last visited Oct. 19, 2021).
[30] Friendica, https://friendi.ca/ (last visited Oct. 19, 2021).
[31] PeerTube, https://joinpeertube.org/ (last visited Oct. 19, 2021).
[32] Plume, https://joinplu.me/ (last visited Oct. 19, 2021).
[33] Bertel King, *What is the Fediverse and Can It Decentralize the Web?,* MUO (Aug. 13, 2021), https://www.makeuseof.com/what-is-the-fediverse-and-can-it-decentralize-the-web/.

Friendica – all without ever leaving their instances, sharing information with either Mastodon or Friendica, or having to use a different service. This system is aptly called the 'Fediverse.'[34]

The advantages of this system are apparent. It ensures maximum user privacy and data autonomy, while not compromising on the core purpose of social media – communicating with others and/or having a wide audience. That being said, FSNs currently enjoy far fewer users compared to conventional social media networks. However, we argue that it is only a matter of time before the technology is more widely adopted. Mastodon currently boasts almost 12,000 instances, and over 4 million active users spread across these instances.[35] The largest instance has over 1 million users, and is operated by the founders of Mastodon. That instance (known as mastodon.social) is connected to over 50,000 instances in the Fediverse – the vast majority of those on Mastodon but also a large number of instances running other FSN software like PixelFed, Friendica, PeerTube, etc.[36] The Fediverse as a whole has over 4.5 million known users as of late 2021.[37]

These numbers may not seem impressive in comparison to conventional social media, but they are still significant - Mastodon had 1

---

[34] James Holloway, *What on Earth is the fediverse and why does it matter?,* NEW ATLAS (Sept. 18, 2018), https://newatlas.com/what-is-the-fediverse/56385/ ; Fediverse, *About Fediverse* https://fediverse. party/en/fediverse (last visited Oct. 19, 2021).

[35] The Federation, https://the-federation.info/#projects (last visited Feb. 01, 2022); Fediverse, https://fediverse.party/en/mastodon/ (last visited Feb. 18, 2023).

[36]Mastodon Instances, https://instances.social/list/advanced#lang=&allowe=& prohibited=&min-users=&max-users= (last visited Mar. 01, 2023).

[37] Kiernan Christ, *What on Earth Is the Fediverse?,* LAWFARE (May. 9, 2022, 11:02 AM), https://www.lawfareblog.com/what-earth-fediverse.

million users by 2017 (a year after release),[38] 2.2 million by 2019[39] and was at 3.7 million by April 2022.[40] This shows a definite pattern of growth. Further, this was achieved despite the adoption of FSN technology not being nearly as easy as signing up on Facebook; a potential user would need to either know how to set up an instance, which involves significant technical knowledge,[41] or how to find and register with one. Both involve significantly more effort than a simple sign up on a single website. As tech literacy and privacy concerns grow, or as governments or bodies such as the EU push for interoperability and other functions uniquely served by FSNs, it can be expected that this number will increase. Further, while ease of access may be a barrier to a regular person, it is quite the opposite for persons with the requisite technical skills or the means of finding them - FSNs being open source allows for any person to use the software to create their own social network within the Fediverse.

A recent example of this is Truth Social, created by former President Donald Trump. Truth Social is an FSN,[42] built on Mastodon's

---

[38] *Id.* at 34.
[39] Tyler Cave, *What is Mastodon and why is everyone talking about it?,* ANDROID AUTHORITY (Nov. 8, 2019), https://www.androidauthority.com/what-is-mastodon-1052151/.
[40] Richard MacManus, *The Fediverse Points to Our Social Media Future, Post-Musk,* THE NEW STACK (Apr. 29, 2022, 8:13 AM), https://thenewstack.io/the-fediverse-points-to-our-social-media-future-post-musk/.
[41] Mastodon, *Running Your Own Server*, https://docs.joinmastodon.org/user/run-your-own/ (last visited Feb. 01, 2022).
[42] Jon Porter, *Trump's new social media app launches on iOS,* THE VERGE (Feb. 21, 2022, 6:54 PM), https://www.theverge.com/2022/2/21/22944179/truth-social-launch-ios-donald-trump-twitter-platform.

code,[43] a fact admitted to by its own makers.[44] Truth Social is thus part of the Fediverse, and interoperable with every other FSN by virtue of this.[45]

All of these factors only serve to show how FSNs, and the underlying technologies that they are based on, are on the rise. How then will the laws apply to them? The Government of India has shown that it is adamant in its goal of regulating social media, but the nature of FSNs make this regulation far more difficult compared to regulating conventional social media. These differences also bring us to the first question we have to ask when considering the applicability of Indian laws related to Intermediaries as they stand with regard to FSNs: Do they even qualify as 'Intermediaries' and, by extension, as 'Social Media Intermediaries'?

B. THE DEFINITION OF 'SOCIAL MEDIA INTERMEDIARIES' AND FSNS

The IT Act, 2000, defines an intermediary as the following:

> *"with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."*[46]

---

[43] Eugen Rochko, *Trump's new social media platform found using Mastodon cod*e, MASTODON (Oct. 29, 2021) https://blog.joinmastodon.org/2021/10/trumps-new-social-media-platform-found-using-mastodon-code/.

[44] Michael Kan, *Trump's social media site quietly admits it's based on Mastodon,* MASHABLE (Dec. 02, 2021), https://mashable.com/article/trump-social-media-mastodon.

[45] Max Eddy, *Trump's Truth Social Can Only Make Mastodon Stronger,* PCMAG (Feb. 16, 2022), https://www.pcmag.com/opinions/trumps-truth-social-can-only-make-mastodon-stronger.

[46] Information Technology Act, 2000, No. 21, § 2(1), Acts of Parliament, 2000 (India) (*hereinafter* "**IT Act**").

It is from this definition that the IT Rules derive their definition of SMIs as a subcategory of intermediaries. The IT Rules employ the following definition:

> *"An intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services"*[47]

The third and final definition relevant to this discussion is for a subcategory of SMIs, known as 'Significant Social Media Intermediaries' ("**SSMIs**"), which are defined in the IT Rules as follows:

> *"a social media intermediary having number of registered users in India above such threshold as notified by the Central Government"*[48]

For the definition of SSMIs, the threshold number of users notified by the Government is currently 5,000,000.[49]

Conventional social media services such as Facebook and Twitter are covered under all three of these definitions, but the lines become slightly blurred with FSNs. At the outset, the initial definition of an intermediary does not seem to cover the operation of an FSN – while a conventional social media service does in fact receive, store, and transmit electronic records on behalf of people, and provides services in relation to such records, FSNs ostensibly do none of these things themselves. The FSN itself is functionally just providing a framework to receive, store and transmit electronic records to the end user, or to other individuals who may

---

[47] IT Rules, Rule 2(1)(w).
[48] IT Rules, Rule 2(1)(v).
[49] Ministry of Electronics and Information Technology, S.O. 942(E) https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf (last visited Oct. 19, 2021).

operate an instance. The FSN does not control the use of any of these functions and does not actually carry them out themselves.[50] Hence, the alternative interpretation leads to absurd conclusions. Considering an FSN as an intermediary would be equivalent to considering the creator of an operating system as an intermediary – they simply provide a framework for computing, which may include activities in the nature of being an intermediary. The creator of an operating system cannot conceivably be held responsible for every action taken by a user of their software.

This disconnect carries forwards into the definition of SMIs as well. The definition in the IT Rules begins with the premise that the SMI is an 'intermediary' as per the IT Act definition, and narrows it down to an intermediary which primarily or solely enables online interaction and sharing of information using its services.[51] It could certainly be said that an FSN, in providing a software framework, enables online interaction and the sharing of information. It is slightly more debatable whether one could be interpreted to be doing this using the FSN's services if the activity is being conducted on a private server, but such an interpretation may not be entirely unrealistic. The problem, however, is that these criteria are prefaced with the requirement of being an 'intermediary', which, as we have seen, is questionable in the context of FSNs.

Even presuming that an FSN could be considered an intermediary, and no other issues arise, the definition of an SSMI also raises a notable concern – When tabulating the number of users, are we to evaluate an FSN

---

[50] Prasid Banerjee, *Moving to Mastodon? You may have missed the social network's point,* LIVEMINT (Nov. 08, 2019), https://www.livemint.com/technology/tech-news/moving-to-mastodon-you-may-have-missed-the-social-network-s-point-11573222761247.html.
[51] IT Rules, Rule 2(1)(w).

on the basis of its overall user base, i.e., including the users of every known instance within its network, or are we going to evaluate each individual instance as its own independent existence? While an FSN overall may have well over 5 million users, individual instances can have as little as 1.

This question also encapsulates the issue of defining an FSN as an intermediary in the first place. While an FSN does not engage in the handling of electronic records itself, the persons who create and operate instances do, having been enabled by the FSNs software. Do we then evaluate the FSN as a whole, or do we evaluate every instance of that FSN on its own? If the goal is to bring FSNs under these definitions, and by extension under regulation, which approach is more viable?

The former possibility is fundamentally impractical. FSN software is open source; the makers do not have control over who may use it to create an instance, much less control over how it is used within an instance. An example of this is the migration of the users of far-right social network Gab from their original software to a version of Mastodon.[52] The founders of Mastodon released press statements denouncing Gab and its users but could not prevent them from using Mastodon. Ultimately, they managed to convince the major instances and their operators to block interaction with instances in the network related to Gab.[53] It is important to note however, while they did manage to effectively isolate Gab, they did so solely because

---

[52] Copia Institute, '*Decentralized social media platform Mastodon deals with an influx of Gab users,* TSF (Jan 13, 2021) https://www.tsf.foundation/blog/decentralized-social-media-platform-mastodon-deals-with-an-influx-of-gab.

[53] TechDirt, *Content Moderation Case Study: Decentralized Social Media Platform Mastodon Deal With an Influx of Gab Users,* TECHDIRT (Mar. 03, 2021), https://www.techdirt.com/articles/20210303/14474346357/content-moderation-case-study-decentralized-social-media-platform-mastodon-deals-with-influx-gab-users-2019.

of the willing support of the operators of the major instances and apps facilitating access to Mastodon instances – by no means could they have forced any person to do so.[54] In differing circumstances, the founders of Mastodon may well have only been able to denounce the migration, as without the support of the users themselves, they are constrained from taking any actual measures. It is worth noting that Gab still operates on Mastodon, even if their servers are isolated.[55] As such, applying any standard in the above definitions to the FSN as a whole would have no impact or meaning since the FSN cannot exercise enough power to fulfil any kind of substantive legal obligation, except perhaps facilitating the necessary software features.

That leaves us with the latter possibility, which seems more tenable, if undesirable (as we will discuss when considering substantive obligations). Instances with multiple users and their operators can be said to both actively fulfil the requirements of the definitions in the Act and IT Rules and have sufficient control over their instances to make substantive obligations possible to fulfil, at least in principle. They are technically handling electronic records and enabling communication, in what is arguably in the nature of service as their operators employ their own private servers to enable others.

However, in the case of instances set up by a single user for themselves, it is arguable whether they could be considered an SMI. This may not be a concern in regular circumstances, as any attempt at communication by an individual would most likely be posted on another

[54] Robertson, *supra* note 13.
[55] TechDirt, *supra* note 53.

instance that has more users (which does fall under the definition and can thus be regulated). However, what happens if the individual has a following? In that case, users from other instances can view what they may be posting on their private instance. Can this be considered an interaction between two or more persons? Is the individual providing themselves with a service? Or can the sharing of their thoughts and making them accessible be considered a service to others? The issue of such instances is notably greyer. We are of the opinion that it would be unreasonable to hold that these individuals are providing themselves or someone else a 'service' simply by creating a space for them to express an opinion on the internet. The viewing of their posts, on the other hand, could be considered an interaction. The greatest issue however is the same as with the FSNs themselves - they are not handling the electronic records of another person in this situation, and thus missing a core ingredient of an intermediary.

In conclusion then, the current law only reasonably provides for instances of an FSN with multiple users to be recognized as SMIs or SSMI (in the event an instance has greater than 5 million users). These instances would all independently bear this status. While the Government of India may not have intended this outcome, and would prefer a wider ambit of accountability, reality remains that this is the reasonable construction of the legislative framework in its current form; this omission is not surprising considering that FSNs were never in consideration when the IT Rules were formulated to govern SMIs, but the lacuna will become problematic should their popularity grow.

The difficulty in governing FSNs could lead to the Government of India taking the stance they did with cryptocurrency;[56] making them outrightly illegal. However, that would be an action with no basis in law - no feature of an FSN is barred under law, and the inability to fit the FSN provider into a workable definition of an SMI is a legislative fault, not a legislative prohibition. Similarly, interpreting the FSN provider into existing law without an appropriate amendment would be an unreasonable expansion of the definitions as they are, and would ultimately serve no functional purpose due to their inherent lack of power.

Having addressed how far FSNs are covered under the current laws in India and to what extent they can be considered SMIs, we arrive at the second question relevant to this discussion: Applying this understanding, what rules become applicable to FSNs and what problems would arise in their enforcement?

C. THE ENFORCEMENT OF SUBSTANTIVE OBLIGATIONS ON FSNS

Assuming that instances with multiple users qualify as intermediaries, and by extension, as SMIs or SSMIs, they face a host of obligations. While the nature and content of these obligations are established and not unique to them in any way, the impact and outcomes of these obligations will vary greatly from a typical intermediary or SMI.

It is important at this juncture to remember that FSN instances are often operated by private persons - they derive no commercial benefit from doing so. Instead, such persons incur costs to run an instance as they

[56] Reserve Bank of India, Prohibition on dealing in Virtual Currencies (VCs), RBI/2017-18/154 (Issued on April 16, 2018).

operate one independently.[57] They may split the maintenance costs with the users in their instance, or they may bear it themselves for the sake of the community they have built. It is also important to note that when we discuss instances with multiple users, as few as 2 users would qualify as 'multiple'.

These considerations are important because the laws are evidently drafted from the perspective of regulating companies, who derive profit from their activities as intermediaries or SMIs, and who have a certain degree of capital available to them. These presumptions fundamentally fail in the context of FSNs, and raise several issues in the process.

Keeping that in mind, obligations on FSN instances arise from the IT Act, 2000, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**"), and the IT Rules. We will address these in order:

1) *IT Act*

The relevant obligations under the IT Act are Sections 67C, 69, 69A, 69B and 70B.[58] Sections 69 and 69A obligate compliance with requests by the Government for access to information, or to block access to information. Section 67C contains the obligation to maintain information for a period and Section 70B prescribes obligations during a data breach. Most of these obligations (such as Sections 69 and 69A) only arise where there is a threat to the sovereignty, integrity or security of India.

---

[57] Mastodon, *Running your own server,* https://docs.joinmastodon.org/user/run-your-own/ (last visited Feb. 01, 2022); Andrew Kvalheim, *Personal Mastodon instance,* GITHUB https://gist.github.com/AndrewKvalheim/a91c4a4624d341fe2faba28520ed2169 (last visited Feb. 01, 2022).

[58] IT Act, §§ 67C, 69, 69A, 70B.

However, compliance with Sections 69, 69A, 69B and 70B of the IT Act would require the operator of the FSN instance to have the technical ability to follow through on monitoring, decryption, blocking and so on. Setting up an instance is an activity that requires a degree of technical skill, but ultimately the software used is not created by the operator themselves - there exists a distinct possibility that their familiarity with its operation is insufficient or that the software itself is not amenable to these requirements and will need modification. It is also of significant concern that all these obligations bear penal consequences. If they lack those skills, they face the risk of imprisonment[59] (whose punishment ranges from three to seven years of imprisonment), as it is unlikely, they may be able to comply even if they are willing.[60]

Any hard-line enforcement of these obligations will then result in dissuading private individuals from making the foray into operating an FSN instance if they lack these skills, raising the barrier to entry and making the technology less accessible, unless developers find a way to make the fulfilling of these obligations easier for potential operators.

2) *2021 IT Rules*

Part 2 of the 2021 IT Rules comprises the primary obligations on SMIs and SSMIs, and the bulk of what FSN instances would be expected to comply with. Rule 3 covers the obligations relevant to SMIs.[61] Rule 4 is

[59] *Id.*
[60] IT Act, §§ 69, 69A.
[61] IT Rules, Rule 3.

unlikely to apply to any instances at this point, as no instance has more than 5 million users.[62]

Several clauses of Rule 3 may be unviable for a large cross section of FSN instances. For example, responding to a take-down order within 36 hours.[63] An operator may not comply with this for a multitude of reasons, ranging from as simple as their internet connectivity failing for that period, to as complicated as bugs in their instance preventing them from doing so. Another example is the obligation to not modify the software to circumvent any law – this may well be outside of the operators' control for a period, as the software is not made by them.[64] While operators can modify software themselves, most will employ the official releases of the open source FSN software they are using, and migrating data to a different software or otherwise rectifying a situation where the open source FSN software violates this obligation may take time.

Other obligations also present challenges. For example, maintaining the data of deleted users and other taken down data for 180 days represents a cost in the form of storage. This may not be an insignificant cost for a private individual who makes no money from operating an instance.[65] Similarly, complex legal documents such as privacy policies may be beyond the ability of most to make themselves, thus requiring engaging a lawyer and bearing that cost as well.[66] Providing information to the Government

[62] IT Rules, Rule 4.
[63] IT Rules, Rule 3(1)(d).
[64] IT Rules, Rule 3(1)(k).
[65] IT Rules, Rules 3(1)(g), 3(1)(h).
[66] IT Rules, Rule 3(1)(a).

and assisting their investigations within 72 hours may also be untenable for the same reasons as complying with a takedown order in 36 hours.[67]

Possibly the most egregious would be the obligation to appoint a Grievance Officer who must respond within 24 hours of complaints of obscene material featuring the complainant, and who must acknowledge any other complaint within 24 hours and act on them within 15 days.[68] This may well comprise a full-time job for the appointed individual depending on the size of the instance. Appointing a person to this role full-time would most likely prove prohibitively expensive for the vast majority of operators, as they derive no commercial benefit from their operating of an instance.

If an instance was to ever become an SSMI with more than 5 million Indian users, the requirements become even harsher. A Chief Compliance Officer and Resident Grievance Officer need to be hired. They must publish compliance reports, create automated tools for identifying certain objectionable material, maintain a physical address in India, and bear a host of other obligations and requirements to operate, all of which represent a cost.[69]

The consequence of non-compliance, in either case, is the stripping of protections afforded to them by the intermediary status and making them liable to criminal action under the Indian Penal Code.[70] Many operators have full-time jobs and bear the hosting costs of an instance solely because of their interest in creating a community. These requirements are a deterrent to FSN instances operating in India or foreign FSN instances

[67] IT Rules, Rule 3(1)(j).
[68] IT Rules, Rule 3(2).
[69] IT Rules, Rule 4.
[70] IT Rules, Rule 7.

accepting Indian users, as these requirements represent a cost and time investment that such an individual may be unable or unwilling to make.

3) *SPDI Rules*

The SPDI Rules have general obligations regarding security and the management of personal data.[71] However, the SPDI Rules apply only to 'body corporates,' as defined in Section 43A of the IT Act, 2000:

"'*body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities*"[72]

This makes it unlikely for these rules to apply to most FSN instances as they are rarely operated by companies or commercial entities; most instances are operated by individuals or informal groups of persons with no real commercial interest. That being said, it is not impossible for a company to operate an instance.

In the event that a company does create an instance, the obligations under the SPDI Rules for the handling of personal data and security are largely possible to comply with, depending on the FSN software used. Regardless, a company may have better means than an individual to modify software for their purposes. Similarly, an individual may be hard-pressed to appoint a Grievance Officer, but a company may be capable of doing so.

4) *The Problem with Enforcement*

We have presumed so far in this discussion of the obligations on FSN instances that they would choose, or at least try, to comply. Another issue that arises, however, is that it is functionally difficult to attempt to

---

[71] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R. 313(E) (India).
[72] *Id.* at Rule 2(1)(c).

enforce these obligations on instances should they choose not to comply. If an instance is hosted in India, action may be taken against them, but what about an instance hosted outside India?

Conventional social media most often operates for-profit. India is a large user base from whom they collect data which they monetize in various ways. They have employees to pay, shareholders to satisfy, and targets to meet. All of these represent interests which the Government can act against, obstruct, or otherwise regulate using the law, in order to control how these companies, behave. None of this is true of FSNs.

FSN software is open source. Any person may operate an instance for any reason, and is highly unlikely to be deriving any kind of monetary benefit from doing so. Should the operator be outside India, they have no reason to comply with Indian law - they do not need to collect data from Indian users, nor are they likely to have any interest in India for the Government to use against them. Any kind of action against such instances would be untenable since there is simply no way to enforce any negative outcome on them. Realistically, the Government could only block Indian users from accessing such services.

This is hardly a solution. It would deny Indian users the benefit of FSN technology. Conventional social media is not a merit good which we seek to promote, with the scope for abuse being established by past events.[73] FSNs represent a viable solution to maintaining the merits of social media, while removing the aspects of conventional social media that users need to be protected from, such as the abuse of their data. The core

[73] Morgan Meaker, *supra* note 10.

tenet of FSNs is privacy and control over one's own identity. By decentralising control, you prevent the kind of abuse the law attempts to address.

However, because the law presumes the existence of SMIs with commercial interests and corresponding resources and capital, it creates a framework where only an SMI with commercial interests and the corresponding resources could conceivably operate. This leaves a vast majority of FSN instances with two choices: expensive compliance for no actual gain or wilful non-compliance. Neither of these outcomes is ideal, and the only loser is the Indian user who may well have benefited from the privacy afforded by FSNs. Instead, the users are forced to use conventional social media, which will inevitably be operated by monetizing their data, and thus, warranting government protection.

This brings us to the last question we must answer: How do we regulate FSNs?

II. THE REGULATION OF FSNS

While FSNs may not be as amenable to regulation, that does not mean they should not be regulated at all. Rather, the approach to FSNs should be one of guiding their development, as opposed to the control method adopted with conventional social media. One of the primary ways the Government of India could engage with the Fediverse is by influencing the technical specifications of FSN software itself. There is a long history of governments influencing the development of technology through means

such as funding research, for example.[74] They could similarly invest in FSN technology, backing developers and researchers working on it and thereby influencing the nature of the technology.[75] For example, FSNs rely on a common 'social networking protocol' in order to communicate with each other;[76] funding research into improved protocols could come with the benefit of ensuring that these protocols are better equipped to enable compliance. This does not happen in the status quo because the law is focused on the intermediaries themselves – the developers of FSN software are not intermediaries, as we have established. Therefore, the burden to adapt is placed on operators of instances who may not have the required skills. This is not a problem for the developers, who can make these adaptations, and are more equipped to do so when engaged with and supported by the Government.

However, given the likely preference of FSN developers to remain removed from governmental interference (given the nature of their work) and the possibility of that kind of interference pushing FSNs away from decentralisation due to the presence of governmental interests, exercising such a macro level of influence may not be wholly viable or desirable.

That being the case, on a more micro level, the Government could simply contribute their own work, such as in the form of plugins[77] that help

---

[74] Jon Pietruszkiewicz, *What are the Appropriate Roles for Government in Technology Deployment? A White Paper with Author's Response to Comments*, NATIONAL RENEWABLE ENERGY LABORATORY (Dec. 1999), https://www.nrel.gov/docs/gen/fy00/26970.pdf.
[75] *Id.*
[76] Matteo Zignani, Sabrina Gaito & Gian Paolo Rossi, *Follow the "Mastodon": Structure and Evolution of a Decentralized Online Social Network*, in PROCEEDINGS OF THE TWELFTH INTERNATIONAL AAAI CONFERENCE ON WEB AND SOCIAL MEDIA, 543, 541-550(2018).
[77] Cambridge Dictionary, Plug-in, https://dictionary.cambridge.org/dictionary/english/plug-in (last visited Feb. 01, 2022).

enable quick compliance with Indian law, or even just enable easier content moderation. Singapore has recently launched the AI Governance Testing Framework and Toolkit providing a means for companies to measure and demonstrate how safe and reliable their artificial intelligence (AI) products and services are.[78] It also launched a Data Anonymisation tool to help organisations better comply with privacy laws.[79] By facilitating the creation of tools for that kind of oversight in FSN software, operators can better comply with take-down notices or other concerns. For example, plugins that facilitate automated flagging of certain types of content (as the Government requires of SSMIs in the IT Rules).[80] In the same vein, automated grievance redressal tools akin to the Online Dispute Resolution (ODR) technology implemented by UPI could make compliance with Rule 3(2) significantly easier.[81] Conventional social media can create such tools for themselves due to their resources (for example, Facebook uses PhotoDNA technology to detect child abuse material on its platform),[82] which FSN operators or even developers may lack, and the Government is uniquely positioned to fill in that gap without necessarily acting as an

[78] PDPC, *Launch of AI Verify – An AI Governance Testing Framework and Toolkit*, https://www.pdpc.gov.sg/news-and-events/announcements/2022/05/launch-of-ai-verify---an-ai-governance-testing-framework-and-toolkit (last visited Feb. 02, 2022).
[79] PDPC, *Data Anonymisation Tool Now Available*, https://www.pdpc.gov.sg/news-and-events/announcements/2022/05/data-anonymisation-tool-now-available (last visited Feb. 02, 2022).
[80] IT Rules, Rule 4(4).
[81] Jaspreet Kaur, *NPCI Orders Banks, Payment Service Providers, Others To Set Up Online Dispute Resolution System,* INC42 (Apr. 14, 2022), https://inc42.com/buzz/npci-orders-banks-payment-service-providers-others-to-set-up-online-dispute-resolution-system/.
[82] Ernie Allen, *Facebook to Use Microsoft's PhotoDNA Technology to Combat Child Exploitation,* MICROSOFT (May 19, 2011), https://blogs.microsoft.com/on-the-issues/2011/05/19/facebook-to-use-microsofts-photodna-technology-to-combat-child-exploitation/.

investor or overseer or in some other capacity that may be seen as motivated or adverse.

Beyond this, the more logistically demanding requirements can be slightly relaxed in order to better suit this context; for example, perhaps permit for extensions of timelines given appropriate circumstances, or limit requirements around grievance redressal and compliance officers. As mentioned, these requirements currently envision compliance by a for-profit entity with significant resources. An individual, even with improved tools, may find it difficult to meet a demand for information under Rule 3(1)(j) within the prescribed 72 hours, or to dispose of a complaint within 15 days.[83] By placing more realistic requirements on operators of FSN instances, you increase the likelihood that they can and will comply. The alternative would discourage the operation of FSNs by anyone without the ability to devote the time and resources to achieve the same degree of compliance required of large companies.

Another avenue is to take the same approach as Mastodon did with Gab – regulate the connections within the Fediverse. Instead of placing complex obligations on individual operators such as retention periods and grievance redressal, the Government can instead focus on roping off problematic parts of the Fediverse, such as those featuring illegal material or facilitating criminal activities. Any operator of an instance chooses the range of other instances they are connected to; ordering operators to avoid a certain subsection of instances would be feasible with the existing tools, and effective at curbing concerns regarding content. This is a fairly simple

[83] IT Rules, Rule 3(2)(j).

requirement to place on instances, and the consequence need only be geo-blocking of URLs[84] of non-compliant instances if they are not based in India, or using legal means if they are.

This would be in line with how FSNs tend to govern themselves. Mastodon has what it calls the 'Mastodon Server Covenant'[85], which requires instances to commit to active moderation against racism, sexism, homophobia, and other objectionable content. While it cannot force instances to comply, they refuse to list non-compliant instances on their server listings,[86] limiting their reach. Wider implementation of this kind of 'Covenant' as a common understanding between FSN platforms is a valid self-regulatory model that could address some concerns regarding content moderation, but ultimately falls short. Firstly, this approach would require a common understanding of what would constitute objectionable content or problematic instances - which is difficult to reach for a collection of platforms that may well have distinctly different priorities. Truth Social, for example, may not see fit to follow something akin to the Mastodon Server Covenant. Secondly, the lack of enforceability of any kind of 'good faith' standard is exacerbated with FSNs, where there is no profit imperative or other motivation that can be inconvenienced to incentivise compliance.

---

[84] Kushaghra Singh et al., *How India Censors the Web,* CENTRE FOR INTERNET AND SOCIETY (May 30, 2020), https://cis-india.org/internet-governance/how-india-censors-the-web-websci; Anisha Mathur, *Explained: Indian and UK laws on pornography as Kundra case has a London link,* INDIA TODAY (Jul. 21, 2021), https://www.indiatoday.in/india/story/explained-indian-and-uk-laws-on-pornography-as-kundra-case-has-a-london-link-1830918-2021-07-21.

[85] Mastodon, *Mastodon Server Covenant*, https://joinmastodon.org/covenant (last visited Feb. 01, 2022).

[86] Eugen Rochko, *Introducing the Mastodon Server Covenant*, MASTODON (May 16, 2019) https://blog.joinmastodon.org/2019/05/introducing-the-mastodon-server-covenant/.

III. CONCLUSION

The Fediverse and FSNs represent the future of social media – one where we can connect with other people through technology, without the pitfalls of monetization and corporate abuse. Of course, no system is free of issues, and any system can be abused by those motivated enough to do so. However, FSNs lower the scope for this to happen by giving people agency over their data, allowing them to keep their online identities in a space they deem safe as opposed to trusting it to an entity which views them as a product.

For this reason alone, it is important that the Government of India adapts to the growth of FSNs. Controlling the power of vast corporations over our freedom of speech is a losing battle, for as much as we regulate them, we continue to let them grow and exert more power and influence. Decentralisation is the key to breaking this power up and restoring it to individuals and communities rather than monolithic entities.

At the highest level, the Fediverse would be a vast network of individuals operating their own private instances, representing their personal identities on the network. This kind of implementation is far off, but it represents the pinnacle of privacy in social media – the online equivalent of in-person interaction, and a worthwhile future to work towards.