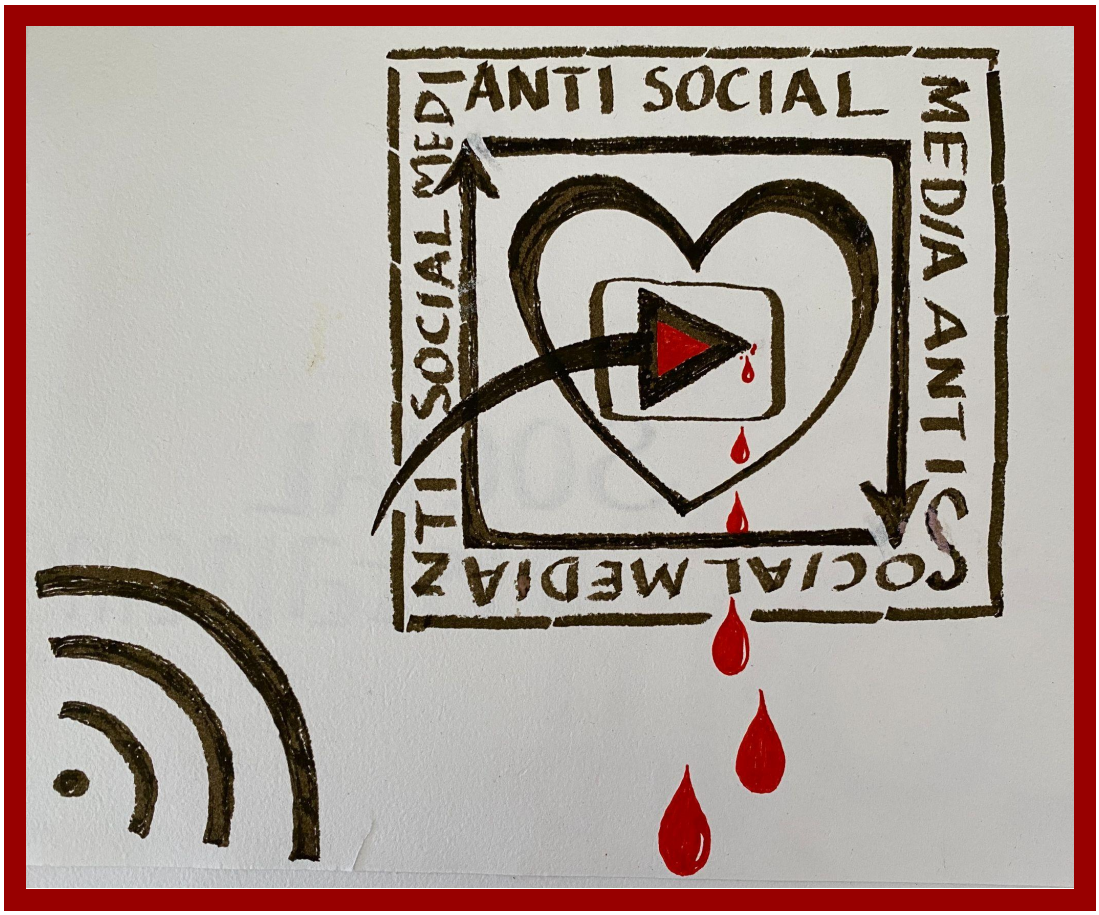
DIGITAL EMPOWERMENT FOUNDATION

WHITE PAPER

SOCIAL MEDIA AFFECTS ALL OF US

The debate over social media needs to be expanded beyond the policy spheres

By Asheef Iqubbal



WHITE PAPER

SOCIAL MEDIA AFFECTS ALL OF US

The debate over social media needs to be expanded beyond the policy spheres

Published by DIGITAL EMPOWERMENT FOUNDATION

Asheef Iqubbal is an independent writer and is a former research associate with Digital Empowerment Foundation

Date of Publication: February 2022

Cover pictures: Digital Empowerment Foundation
Author: Asheef Iqubbal

Digital Empowerment Foundation
House no. 44, 2nd and 3rd Floor (next to Narayana IIT Academy) Kalu Sarai (near IIT Flyover)
New Delhi – 110016
Email: *def@defindia.net* | URL: *www.defindia.org*

DIGITAL EMPOWERMENT FOUNDATION

WHITE PAPER

SOCIAL MEDIA AFFECTS ALL OF US

The debate over social media needs to be expanded beyond the policy spheres

By Asheef Iqubbal

India enacted Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) on 25 May 2021 that regulates user generated content and is being criticised for directly unleashing comprehensive attacks on freedom of expression, an essential part of the functioning democratic society. The first part of the rules aimed at governing social media intermediaries, the second part at the over-the- top (OTT) streaming services, and the third part at online news platforms. This piece will focus on how free speech, civic participation, and democratic functioning are being redefined from the perspective of journalists, activists, and communities within the context of new social media regulations, as the rules provide ambiguous and broad grounds such as "morality", "decency", and "defamation" to classify speech as "unlawful".

The rules mandate multiple obligations on social media platforms such as social media firms will have to coordinate with the law enforcement agencies, taking down of that content within 36 hours upon actual knowledge; handing over users' information; mandating traceability that will functionally undermine the end-to-end encryption; use of automated machine learning in digital sphere for grossly harmful content; putting out monthly compliance report; appointment of officer in India; and if the officers do not cooperate with the enforcement agencies they could be prosecuted. Reading these rules in tandem with the already shrinking space for freedom of speech, expression, and assembly under the current ruling dispensation paints a scary picture for the future of online democratic participation.

Amplifying The Fear Of Opaque Content Removal

The government has tried to silence the dissenting voices on the digital public spheres that include lodging cases for social media posts, shutting down the Internet services, and blocking content from the public view. Content removal requests from 2018, the

year in which Intermediary guidelines were introduced, to 2021, the year in which rules have been enacted tells a story of increasing control of the state on social media platforms. The transparency report of Twitter of 2018 shows that it received 913 legal demands for content removal which includes 19 court orders and 894 other legal demands and compliance rate was zero percent. In 2019, it received 1286 legal requests for the content removal out of which the court's order was 15 and compliance rate was increased to 36.7 percent. In 2020, legal demands rose to 2772 out of which only 4 were from court and compliance rate was 13.8 percent.

Facebook Transparency Report of 2018 shows that it has received a total 37.4 thousand government requests for users' data and Facebook produced some data on 53 percent case. While in 2019 it received 49.4 thousand requests and data produced in some cases were 55.5 percent, in 2020 it received 75.9 requests and some data produced were 51 percent. Except for the increase in legal requests from the government and India being in the list of top few countries in requesting for content removal, transparency reports of these two major platforms Facebook and Twitter say very little about the scale of censorship as the reports do not show the kind of content that are being requested for the removal. Government has constantly denied the disclosure of the orders on the grounds of public order and national security that means a chance to be heard by the content creator is disparate, hence violates the principle of natural justice.

The reports available in the public domain do not produce much confidence about the government's order as well. Between 2018 and 2021 the only instance that the government has requested for the removal of tweet is of Tejaswi Surya's tweet of 2015 which linked terror to Islam, other than that almost every request seems to be an effort of controlling the narrtive. For example, during the second wave of COVID–19 pandemic in which thousands of people died, the government requested Twitter to remove 52 tweets. A closer look at these tweets shows that largely it appeared to be straightforward news, political commentary and criticism of the government in handling COVID–19. Twitter revealed this information on Lumen, a database that keeps track of global government orders around online content. Similarly, the government asked Twitter to block more than 250 handles including *The Caravan*, a prominent news magazine, under 69A of IT Act for using controversial hashtags during farmers' agitation which the government found inflammatory and could lead to public order in the aftermath of republic day violence.

After public pressure mounted on Twitter for violating free speech, suspensions were revoked after a couple of hours. After revocation of the accounts, Twitter employees were threatened by the government of being put behind the bars unless it blocked them

again. News reports available on content removal are largely about Twitter, as unlike Facebook, Twitter reveals the government order to Lumen until it is prohibited to do so. Facebook's record in protecting free speech and propagating hate has been questionable as well. In February 2020, when communal violence broke out in the parts of North-East Delhi, in the wake of an amendment in the Citizenship Act in which 52 people were killed, Facebook was instrumentalized to propagate hate against Muslims –– India's largest religious minority group. Later, a news story revealed that Facebook did not take down incendiary speeches due to the fear of colliding with the ruling establishment in the country –– the Bharatiya Janata Party. Interestingly, people from the ruling establishment continue to enjoy relaxations under the same provision of IT Act, 69A, despite spreading misinformation or even hate speech on social media platforms.

Above examples show that social media platforms have systematically failed to protect human rights and values of free speech on their platforms which has often translated to offline violence and polarisation of the society. This is because of the economic functionality of the platforms –– generating revenues through users' engagement that includes everything from hate speech to fake news. This has serious implications on civic and political engagement as IT Rules, 2021 can be leveraged by the state to exert disproportionate power over the social media companies that are facilitative to the democratic participation. In addition to the content removal, the bottlenecks in unfettered participation in democratic culture and accessibility of information has been the pathological response of Internet shutdown in order to maintain 'public order'. In 2020, 70 percent of the global shutdowns have been recorded in India. India continues to top the list of shutdowns since 2016 which include one of the longest outages in Jammu and Kashmir, when the government stripped autonomy of the state.

Promoting Opacity Rather Than Transparency

The debate between technologists and law enforcement agencies over encryption is not a new one. On one hand, there are privacy advocates who believe people should be able to communicate online without any sort of surveillance. On the other hand, there are law enforcement agencies and lawmakers, who believe encryption makes it impossible to track criminal activity, such as child predators, terrorists, among others. In the wake of multiple incidents of lynching fuelled by rumours on WhatsApp occurring in different parts of the country, a major debate over encryption in India began in 2018. The central government notified the draft of the Information Technology (Intermediary Guideline) Rules, 2018 for public consultation by the Ministry of Electronics and Information Technology to review the existing Information Technology (Intermediary Rules), 2011. The 2018 draft argued in favour of traceability of the original content

creators in order to curb fake news and obscene content, and to prevent the misuse of social media platforms.

Rule 4(2) of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 also requires significant social media intermediaries –– primarily those providing messaging services –– to identify the "first originator" of the information sent via electronic device. Rule 2(v) defines significant social media intermediaries as an intermediary having a certain threshold of registered users in India. The implementation of traceability on significant social media intermediaries, which will include almost every messaging platform in India, end-to-end encrypted platforms evokes the fear of users' privacy breach. The case of tracing original content creators is already going on in the Supreme Court of India. Animal welfare activists Antony Rubin and Janani Krishnamurthy filed petitions in the Madras High Court for linking Aadhaar Cards –– a 12-digit unique biometric ID –– to social media accounts to improve cyber security. While adjourning the hearing, Madras High Court clarified that it was no longer considering the original petition to link Aadhaar with social media accounts. The court stated that Aadhaar can only be mandated in delivering social welfare programmes, and instead of linking it with social media, its focus was on improving coordination between law enforcement agencies and social media companies.

The Madras High Court asked Prof V Kamakoti of IIT Madras, also a member of the National Security Advisory Board (NSAB), to submit a report on the feasibility of messages on WhatsApp being traced. In late July 2019, he informed the court that original sender can be traced on end-to-end encrypted social media platforms, by suggesting that an information tag must be added to the message that was originally sent, so when it is eventually forwarded, the original person's information details would be attached along with it. Later, the case was transferred to the Supreme Court, where WhatsApp and its parent company, Facebook, is a party. However, social messaging platforms such as WhatsApp –– who use the 'Signal protocol end-to-end encryption' –– have long argued that mandating traceability will undermine users' privacy. According to WhatsApp, their end-to-end encryption ensures that only the sender(s) and the recipient(s) can read the exchange of content between them, and nobody in between, not even WhatsApp or their parent company Facebook, can access that content. A third party in this context means any organisation that is not the sender or recipient, directly participating in the conversation.

Moreover, WhatsApp stated in the Madras High Court that it only has little information about the sender, which includes phone number, name, device information, app version,

start date/time, connection status, last connection date/time/IP, email address, and web client data. WhatsApp also has information about all the contacts of a user and names of all the groups they are part of, but the Madras HC submission did not include it. Signal, another instant messaging app, stated that it only has the date on which the account is created and the last connection date because it does not collect any other data. However, as per the new rule, the government has not categorically asked for breaking of the end-to-end encryption; it has just defined the information it wants under Section 69 of Information Technology Act, 2000 (IT Act) or judicial order — the first originator — without describing the method and offering adequate procedural safeguards. Moreover, operatively, mandating traceability may undermine end-to-end encryption on significant social media platforms. WhatsApp has filed another lawsuit in Delhi high court by challenging the constitutional validity of the IT Rules, 202.

If the originator of the content does not reside within Indian territory, the first originator in the territory of India will be considered the original content creator. This is problematic because to trace this, platforms would have to collect the metadata of the whole conversation, undermining the end-to-end encryption, and subsequently, the safety of the conversation. This also means that WhatsApp would have to provide one service to the Indian residents and other to non-Indian residents –– where traceability is not mandated. Regulations coercing significant intermediaries, especially those who provide messaging services, to re-engineer their architecture of end-to-end encryption, would have significant repercussions on free speech, and fundamental constitutional and human rights. As per the new rule, platforms have to hand over users' information as well to enforcement agencies, if they demand it. Apart from impacting direct freedom of expression, one of the unintended consequences of such regulations would be the promotion of *opacity* rather than *transparency* as broadly worded provision of Section 69 of IT Act would allow law enforcement agencies to bypass the judicial process.

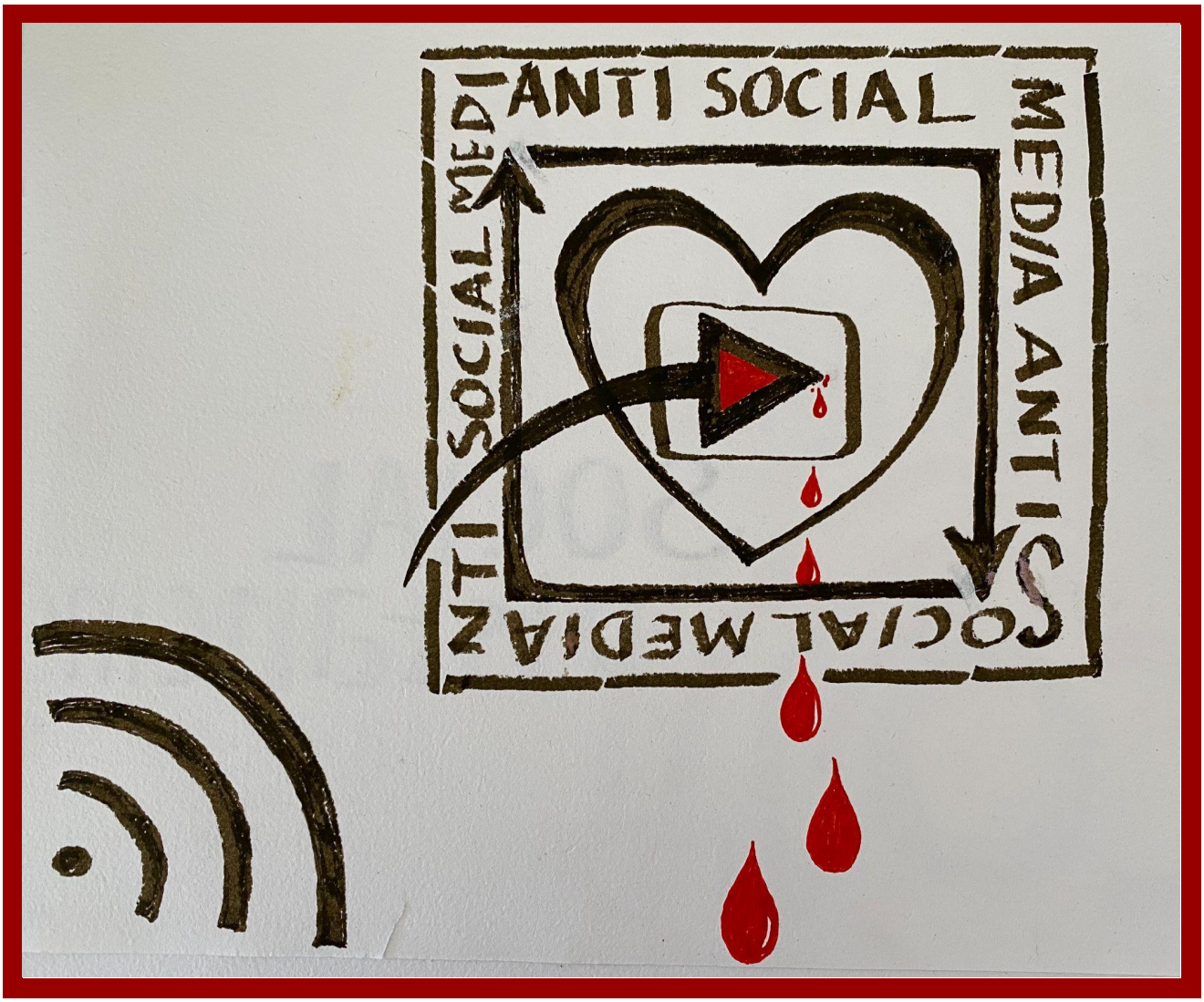
Perspective From The Ground

These fears were reflected during the interviews among journalists, activists and communities that were conducted in the context of proposed intermediary rules, similar to the enacted one. Surya Prakash, a labour rights activist in New Delhi said, "Even now when I try to post something related to labour rights on Facebook, the platform does not allow citing that the post goes against their community standards. And, we all know what kind of post against one section of the society is relentlessly being shared on social media and nobody cares, neither the government nor Facebook. Such rules must be opposed as it will empower only the government and not the citizens." Similar apprehensions were raised by a Lucknow based journalist, Ranvijay Singh. He said, "What would happen when the government starts considering every

dissenting voice as anti-national? Even uploading news on social media platforms would become difficult."

Journalists fear that reporting on sensitive information like violation of human rights and corruption of heavyweight political leaders that requires freedom to seek, receive and impart any information without interference would become difficult as the government is forcing the platforms such as Signal and WhatsApp, a primary messaging app, to enable the traceability. Parth MN, an independent journalist based in Mumbai siad, "If any journalist would be investigating stories on sensitive issues that the government wants to restrict, their sources can be traced [If encryption is compromised]. It would endanger the lives of both journalist and source. This is akin to China's model of surveillance." India acceded to International Covenant on Civil and Political Rights (ICCPR) by affirming its commitment to the freedoms laid down in the Covenant. Article 19 ICCPR ensures unfettered communication without fear of being watched but new rules are violated by opening up a scope through traceability, and by putting greater obligation on social media firms to police their platforms.

The United Nations Special Rapporteur on Right to Freedom of Speech and Expression has already raised apprehension over new rules by citing that it will breach users' free speech and privacy, a fundamental right declared by the Indian Supreme Court. Similar apprehension was raised among three villages of Haryana, Uttar Pradesh and Rajasthan. A shopkeeper in Khaur village in Uttar Pradesh said, "If WhatsApp compromises its encryption, then what will happen to our privacy! It should never be allowed to happen. What we talk about in personal life, it is nobody's business to read or keep an eye on. Even the Supreme Court has said that privacy is a fundamental right, so, nobody should take it away." India needs to discuss the role of social media firms and governmental regulation around it at every institutional level –– political to social –– not only in policy spheres, as it has opened several cracks in Indian democracy and are already affecting the everyday expressions of Indian people. This includes religious polarisation, fake news, healthcare. If the relevant people fail to expand the debate over the role of social media in the democratic lives, it will be futile to think that either the government or social media companies will act to protect the interests of common people.



WHITE PAPER

SOCIAL MEDIA AFFECTS ALL OF US

The debate over social media needs to be expanded beyond the policy spheres

Published by DIGITAL EMPOWERMENT FOUNDATION

Asheef Iqubbal is an independent writer and is a former research associate with Digital Empowerment Foundation

DIGITAL EMPOWERMENT *foundation*