India's New Intermediary Guidelines

The Gloves Come Off in the Assault on Civil Liberties

Tanmay Singh & Abhinav Sekhri

01.06.2021 doi: 10.17176/20210602-003803-0

The past week has been remarkable, as the Indian Government has found itself at loggerheads with both WhatsApp and Twitter. At the heart of these disputes are the Intermediaries Guidelines and Digital Media Ethics Code 2021 (or "IT Rules 2021" for short). In their justification, the Government accused Twitter of being "invisible" in its commitment to the Indian people, and WhatsApp of being "misguided" in its opposition to new government measures.

The IT Rules 2021 came into force in February and have significantly altered the intermediary liability landscape, as well as the publication of news and media content on the internet, over streaming platforms such as Netflix and Amazon Prime. The Rules have created a set of additional due diligence obligations for all intermediaries, with even more onerous requirements for "significant social media intermediaries" (SSMI) [Defined through Rules 2(1)(v) and (w) and notified as platforms with more than 5 million registered users], such as Twitter and WhatsApp. The consequences of non-compliance with the regulations are severe: losing the traditional protection from liability which intermediaries enjoy [Rule 7].

May 26 marked the expiry of the three-month grace period offered to SSMIs. They may now face liability for content hosted on their platforms. Both Twitter and WhatsApp have thus far played a cautious hand; putting out aggressive statements, including a possible litigation, while slowly moving to comply with the new norms. Which prompts the question: Just what are these new Rules doing anyway? In line with the broad consensus, we argue that the changes brought about the IT Rules 2021 are deeply problematic on the whole. Foremost, they are a tool to vest more power over speech online with the executive.

The Notice and Takedown Regime

Prior to the IT Rules 2021, the notice and takedown regime required that intermediaries *respond* to requests for takedown within 36 hours of being made aware of offending content on their platforms, by way of official notices or court orders. While the 2011 Rules required that intermediaries "act" within 36 hours, the Supreme Court of India which limited this requirement, in the landmark *Shreya Singhal*judgment [(2015) 5 SCC 1], to only require a response within such time.

The Supreme Court held that a hasty notice and takedown regime would cast a chilling effect on free speech and expression online. It would spur self-censorship by intermediaries in efforts to avoid potential liability, and place them in the position of policing the internet – as "deputy sheriffs" as argued in the German context. Given that "borderline" speech is often going to be critical of existing power structures, the costs of the chilling effect on democratic participation was decisive for the Supreme Court. Very recently, in June 2020 the French High Court had also struck down legislation on similar grounds.

The IT Rules 2021 have taken a hammer to this setup and, contrary to existing precedent, reinstated the requirement for intermediaries to "remove or disable access" to the content within 36 hours of having actual knowledge of a court order or government notice. The scope of prohibited content is very vast: not only does it cover content allegedly prejudicial to national security but also vague notions of "public order", "decency" or "morality" [Rule 3(1)(d)]. In some cases, such as content which *prima facie* suggests nudity, intermediaries are required to take action to remove content within 24 hours [Rule 3(2)(b)].

It cannot be understated how big a problem this is and why the Supreme Court was convinced to limit the requirement in 2014. Rule 3(1)(d) confers potentially boundless discretion to administrative officers to seek takedowns of what *they think* is prejudicial to *their* notions of public order or decency. This effectively renders exercise of a basic civil liberty subject to the pleasure and perspective of mid-level bureaucrats. This boundless discretion, in turn, casts a signaling effect on the platforms and sets the standard for the kind of moderation they should exercise to avoid potential skirmishes with law enforcement.

Another change brought about the IT Rules 2021 is the creation of the 'SSMI' category of intermediaries. As mentioned above, an even stricter set of regulations, including a requirement to have a strong domestic presence, will govern SSMIs. Recognizing that big platforms like Facebook ought to be governed differently is fine. Curiously though, the IT Rules abandon this logic in the same breadth and empower the executive to nominate *any* social media platform as an SSMI, if an undefined "material risk of harm" can be demonstrated to state sovereignty, foreign relations, or public order [Rule 6]. This appears an attempt to give additional legal options to the government, in the wake of the ongoing disputes with China, which resulted in a ban of TikTok in India. However, as should be clear by now, the outcome is to vest arbitrary discretion with the authorities, disproportionate to the perceived problem at hand.

The chilling effect on free speech is not only to be measured toward big platforms like Twitter. After all, Twitter and alike at least have the resources to comply with the tough regulatory measures with quick turnarounds. Complying with the new measures is likely to prove a bridge too far for many smaller platforms, let alone the added obligations which may follow for platforms which are close to the 5 million subscriber mark for SSMIs. or are arbitrarily notified as such by the government due to state interests. This either exposes smaller platforms to liability or potential shutdowns altogether, which further reduces the democratic and horizontal construct of the digital space into a playing field largely controlled by big tech.

Complying with Law Enforcement

Intermediaries are now required to comply with a host of new measures to further law enforcement interests. This includes (i) a requirement to store offending content removed following a takedown request as well as registration data [Rules 3(1)(g) & (h)]; and (ii) complying with law enforcement requests for information within 72 hours of receiving a request. Both are problematic from a privacy perspective, on account of a separate issue of India not having any personal data protection regime in place.

The most controversial new requirement in this regard, however, is that of obliging SSMIs such as WhatsApp to enable identification of "first originators" for messages pursuant to a law enforcement request. WhatsApp has argued that compliance with this requirement entails weakening, if not fully breaking, the end-to-end encryption that has come to define its terms of service. This constitutes an impermissible infringement of the privacy of its millions of users.

Perhaps sensing the obvious threat to privacy and citizens' acceptance of E-2-E encryption as standard, the Government has meekly stated that the Rules don't explicitly compel breaking encryption, and that the method of compliance is up to the entity in question. It is doubtful whether there are any solutions other than to break encryption. Even so, it is important to remember that the privacy jurisprudence in India is still relatively nascent. It was only unequivocally recognized as a fundamental right by the Indian Supreme Court in 2017. The Court batted for a proportionality analysis but at the same time introduced a state interests' exception for law enforcement purposes, and it is fair to say that the contours of the latter are rather fuzzy. Going by the public statements made thus far, it is likely that in any potential litigation this will be the foremost argument that the government adopts, claiming that it needs first originator data to book those spreading hate speech and fake news through platforms.

A more technical but equally pertinent objection to Rule 4(2) might lie in free speech grounds. As it stands, the potential grounds upon which law enforce-

ment may request this data exceed the specified grounds for limiting exercise of free speech under Article 19(2) of the Constitution, and thus open the door for vague requests. Even if courts somehow do place law enforcement requirement as one of the justified grounds for limiting speech, the measure must satisfy the requirement of being a "reasonable restriction" towards achieving the goal. If the only way to identify first originators would be through practically removing E-2-E encryption, it would arguably make for an unreasonable restriction on the exercise of speech by all persons.

Conclusions

The Electronic Frontier Foundation nicely captures the kind of sensitive approach required when going down the road of "reforming" intermediary liability regulations:

As a general matter, the best starting point is to ask: "Are intermediary protections the problem? Is my solution going to fix that problem? Can I mitigate the inevitable collateral effects?" The answer to all three should be a firm "Yes." If so, the idea might be worth pursuing. If not, back to the drawing board.

Incitement to violence, disinformation, hate speech – these are equally problematic, no matter the platform. They cause irreparable harm to individuals and naturally raise calls for regulation and accountability. But were intermediary protections *the problem?* The salience of this question is heightened when we consider a country like India. Time and time again, it is the executive that has been found wanting in its response to these very problems of hate speech and disinformation, being accused of biased enforcement which favors political interests and brutalizes religious minorities [see *here*, *here*, and*here*]. Indeed, it is this perception which prompted Twitter to publicly condemn "intimidation tactics" being used by the state, when police officers visited Twitter offices after it tagged posts of ruling party leaders as "manipulated media".

This is why it is difficult to take the government's claims, that the IT Rules are designed to foster the interests of free speech and users' safety, seriously. It is much more likely that the enormous powers to control speech, either directly or by proxy, which will now rest with the executive, are going to be used to safeguard vested interests and efficiently, aggressively, quell forms of dissent.

Disclaimer: The authors are part of the legal team advising the petitioners in a challenge to the IT Rules 2021 pending before the High Court of Kerala, in Livelaw Media Pvt Ltd v. Union of India & Anr.

ABOUT THE AUTHORS

Tanmay Singh
Tanmay Singh is the Litigation Counsel at the Internet Freedom Foundation. He specialises in strategic litigation around digital rights issues.Tanmay Singh is the Litigation Counsel at the Internet Freedom Foundation. He specialises in strategic litigation around digital rights issues.
Abhinav Sekhri
Abhinav Sekhri is a legal writer and lawyer practising in New Delhi, India. He specializes in criminal law, evidence, and procedure.Abhinav Sekhri is a legal writer and lawyer practising in New Delhi, India. He specializes in criminal law, evidence, and procedure.

SUGGESTED CITATION

Singh, Tanmay; Sekhri, Abhinav: India's New Intermediary Guidelines: The Gloves Come Off in the Assault on Civil Liberties, Verfassungsblog, 01.06.2021, doi: 10.17176/20210602-003803-0.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20210602-003803-0.