TAKSHASHILA INSTITUTION

Economic Implications of WhatsApp's Lawsuit against the Government of India

Atish Padhy & Suchir Kalra

31st May 2021

Issue Paper 2021-01

Executive Summary

India's new Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules (IT rules, 2021) enforced a requirement on platforms that provide messaging services to trace the "first originator" of unlawful content. This presents fundamental difficulties for encrypted platforms. Challenging this requirement, WhatsApp filed a lawsuit against the Government of India in Delhi High Court on 26th May 2021.

In this document, we attempt to assess the likely implications of the lawsuit on the instant messaging market in India. In our assessment:

1. If the court rules in favour of WhatsApp, the status quo is likely to be maintained, with a possibility of WhatsApp further consolidating the market.

2. If the court rules against WhatsApp, WhatsApp can either choose to comply and remain in India or leave. If it complies, it is likely to remain the dominant player. Platforms that are end-to-end encrypted, meanwhile, might be blocked if they are unwilling to comply.

3. If WhatsApp leaves, at first, there would be a void in the market. Until there is a standardised platform of communication, there could be a fall in consumer surplus.

4. The traceability requirement might not serve the intended public interest benefit.

This is an assessment prepared by the authors for discussion and debate. It does not reflect Takshashila's policy recommendations.

I. Background

On 26th May 2021, WhatsApp sued the Government of India over the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules (IT rules, 2021), stating that compliance with the traceability requirement under rule 5(2) would require breaking end-to-end encryption of messages and undermine the Fundamental Right to Privacy of Indian citizens.

The architecture of end-to-end encrypted platforms is such that both the content of a message and the sender's identity is visible only to the receiver. For instance, suppose there is a particular message 'A' that is flagged. To trace the first originator of 'A', the digital intermediary would have to develop techniques to figure out the entire chain of transmission of A. In turn, this might lead to a situation where in order to determine the sender of a particular message, messages sent by a likely much more extensive set of users that happen to be in the chain may need to be decrypted.

The Ministry of Electronics and Information Technology (MeitY), in a press statement, has stated that "It is in public interest that whoever started the mischief leading to such crime must be detected and punished. We cannot deny as to how in cases of mob lynching and riots etc. repeated WhatsApp messages are circulated and recirculated whose content are[*sic*] already in the public domain. Hence the role of who originated[*sic*] is very important."

The case is pertinent not only to the fundamental right to privacy but also has significant effects on the instant messaging (IM) market and the larger technology ecosystem in India.

II. Why are rule 5(1) and Rule 5(2) of the IT Rules, 2021 crucial?

The IT rules, 2021 impose several regulations on digital intermediaries in India, arguably the most stringent of which apply to "Significant Social Media Intermediaries", defined as having more than 5 million registered users. Among these regulations is rule 5(2), which states that social media intermediaries providing messaging services must enable the identification of

the first originator of a message when requested to do so for law enforcement purposes. This presents significant challenges for end-to-end encrypted services, like WhatsApp and Signal, which must reengineer their platforms to comply with the regulations.

In addition to having a physical address in India, under rule 5(1), Significant Social Media intermediaries are required to establish an entire compliance team, which would include:

a) A Chief Compliance Officer, who would be liable if the intermediary fails to comply with the IT rules

b) A team of nodal contact persons who will coordinate with law enforcement authorities

c) A Resident Grievance Officer, who would be based out of India.

III. What might happen next?

In our evaluation, the following broad scenarios could emerge:

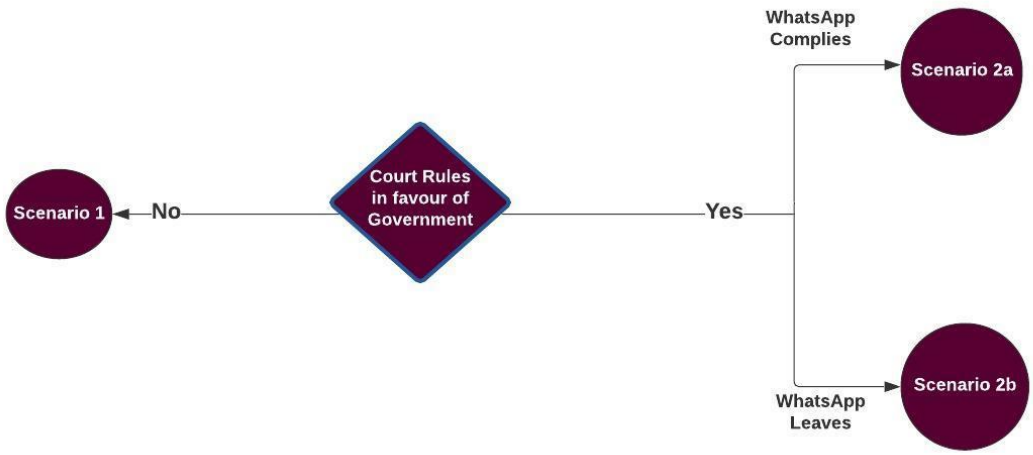


Figure 1: Possible outcomes of WhatsApp's lawsuit against the government

Scenario 1 - Court rules against the Government

Our Assessment: The status quo will be maintained with a possibility of WhatsApp further consolidating the market.

In the Puttaswamy judgement in 2017, the Supreme Court held privacy as a fundamental right that could only be infringed upon when the extent of infringement is proportional to the need for infringement. At the outset, decrypting unrelated messages and messages of multiple parties in a chain of messages can often be disproportionate. Hence, it is possible that the court might strike down the 'traceability' requirement.

But in reviewing and evaluating the case, the court might restrict itself to the traceability requirement and not review the other stringent requirements under the IT rules. As of 29th May 2021, WhatsApp, Facebook, Google, Telegram and LinkedIn have complied with the requirements under rule 5(1) and have shared the details of their Chief Compliance Officer, Nodal Officers of Contact, and Grievance Redressal Officer.

It is thus likely that even if the traceability requirement is found unconstitutional, the remaining rules will continue to apply, resulting in a highly regulated market since the costs of compliance with requirements other than traceability could potentially be reasonably high. Additionally, in the light of Delhi Police's recent "raid" of Twitter's India office, the requirement under rule 5(1) that an intermediary should have an address in India, and a Resident Grievance Officer, could be used to coerce platforms to comply with certain government's orders.

In our assessment, the status quo will likely be maintained, with WhatsApp continuing to remain the most popular player. Yet, there is a possibility of WhatsApp consolidating the IM market further. This will be due to the following reasons:

1. Being the dominant player in the IM market, driven by network effects, the switching costs[1] for a user to move from WhatsApp to another platform are high. For instance, despite its controversial privacy policy update this year, users still continued using WhatsApp. This is evidenced by the fact that WhatsApp did not see a drop in usage, even as Signal and Telegram saw record downloads, since users often use multiple platforms simultaneously.
2. WhatsApp has begun to generate some revenue through its WhatsApp Business API, planning to use its "status" feature for advertising and is attempting to integrate more closely with the larger Facebook advertising machinery by sharing non-messaging data, as indicated in its controversial privacy policy update earlier this

[1] Switching costs refer to costs that users might face while shifting from a product or service they regularly use to another. Examples of such costs are the costs of inconvenience and learning to use the new product with ease, lack of accessibility, limited features, etc. A simpler way to understand this is as user inertia, wherein they will prefer to continue using the product that they already use.

year. It is estimated that WhatsApp could generate anywhere between $5 billion to $15 billion for Facebook Group in the coming years.

3. With the business API, WhatsApp is increasingly becoming the platform of choice for businesses. During a pandemic when lockdowns are intermittently imposed, ease of communication between businesses and customers is a great advantage to both the business and the customer. This further increases the switching costs of moving away from WhatsApp.

Scenario 2(a): Court rules in favour of the Government, and WhatsApp complies

Our Assessment: WhatsApp is likely to remain the dominant player. However, other platforms without end-to-end encryption standards are likely to grow. Platforms that are end-to-end encrypted, meanwhile, might be blocked if they are unwilling to comply and develop a mechanism to decrypt messages to trace the first originator.

With over 400 million users, India is WhatsApp's single largest market, which it has been attempting to integrate more closely with Facebook's larger advertising structure. This could be enough reason for it to comply with the judgement. Given the size and importance of the Indian market to Facebook, it may attempt to create an India-compliant version of WhatsApp; however, it is unclear how/whether this may happen.

If WhatsApp does comply and remain in India, it will likely continue to be the dominant player. As discussed in Scenario 1, the switching costs for users to move from WhatsApp to another IM platform are relatively high.

The effects on other players will not be uniform. Within the IM market in India, there exist platforms with a variety of encryption standards. Those that do not have default end-to-end encryption should find it easier to comply with the traceability requirement without significant reengineering and grow as a result. Telegram is one such platform, where regular chats between two users and group chats are secured by cloud encryption and only secret chats between two users are end-to-end encrypted. Unlike end-to-end encrypted data, cloud encrypted messages are stored in servers and are thus accessible.

On the other hand, platforms whose USP is their high privacy and security standards, such as Signal, might be unwilling and unable to comply with these regulations. If the traceability rule is enforced and Signal disagrees/is unable to trace the first originator, it might be blocked by the government for noncompliance.

Scenario 2(b): WhatsApp leaves the Indian Market

Our Assessment: At first, there would be a void in the market. Until there is a standardised platform of communication, there could be a fall in consumer surplus. However, with potential government backing and network effects, there is a possibility of a homegrown player dominating the market.

If traceability is upheld by the court and WhatsApp creates a mechanism to trace first originators, the decision might set a global precedent. If WhatsApp agrees to comply with the traceability rule in India, it might not have bargaining power if similar regulations are enforced in other countries. This is crucial given the concerted efforts by governments globally to clamp down on end-to-end encryption. As MeitY's press release regarding WhatsApp's lawsuit notes, "In July 2019[i], the governments of the United Kingdom, United States, Australia, New Zealand and Canada issued a communique, concluding that: 'tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can gain access to data in a readable and usable format.'"

WhatsApp's departure would leave a void in the market, which other players, especially those without end-to-end encryption, would attempt to fill. Among other alternatives, we might witness the revival of SMS. But in our assessment, a crucial factor that might determine the future of the IM market is India's Made in India and *AtmaNirbhar Bharat* policies.

In the past, there have been instances when the government has given preference to homegrown IM platforms, perhaps due to the greater bargaining/regulatory power that it has over them, as opposed to global players. For instance, JioChat was the only IM platform on the Whitelist for a week during the restrictions on internet connectivity in Kashmir in 2019-20. Moreover, the government has developed an IM platform in an attempt to enter the market.

This preference is already playing out in the social media market. Twitter, for instance, has a homegrown competitor Koo, which has garnered 6 million Indian users in over one year of operation. Given the increasing tension between the government and Twitter, along with the fact that Koo has already complied with the IT rules, one can expect an arbitrary imposition of the regulations in a way that benefits the growth of the homegrown app. Several ministers have expressed their support for Koo in the past.

Therefore, it is likely that the government might assist certain homegrown IM platforms with regulatory relaxation/preference, resulting in the emergence of a dominant "Made for India" player. However, the security and the acceptability of such a platform by the

population are likely questionable due to the platform's close relationship with the government and the consequent concerns of extensive data sharing with the government.

Government backing and network effects will likely lead to eventually the emergence of one or two dominant players in the market. Given the regulatory incentive to build weaker encryption mechanisms, the dominant players could exploit this opportunity by heavily monetising user data.

Until there is a standardised platform of communication (similar to WhatsApp), there is a likelihood of macro-level effects on India's economy in the short run. WhatsApp, being a standardised communication platform accessed by a large user base globally, including businesses, creates great value by reducing friction in communication and collaboration. A standardised and widely accepted form of communication can improve work efficiency, lower costs and thereby help increase productivity.

Therefore, if WhatsApp departs, especially at a time when businesses, schools and users rely on the internet to communicate and work, there is a potential of higher transaction costs, lower levels of productivity and structural changes in the day to day routine of WhatsApp users in India. This could contribute to a short term economic slowdown and a fall in consumer surplus until there is a transition to an IM platform that has similar network effects.

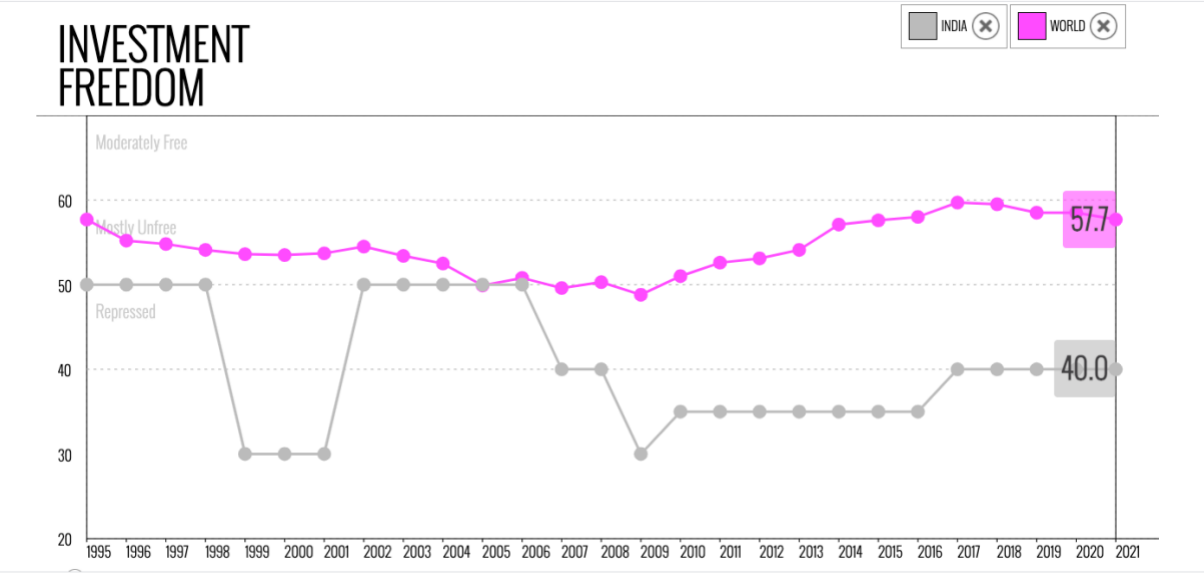
Broader consequences of the IT rules

Irrespective of whether WhatsApp decides to comply with the IT rules or leave the market, if the court rules in favour of the government, there could be several changes in how digital intermediaries operate.

Social media platforms that provide messaging services as a part of their larger product, such as Twitter and Instagram, and Workspace applications like Microsoft Teams, would also have to comply with all the IT rules, including the traceability requirement. Many of the challenges we have identified for the IM platform market would also apply to the social media market. Given the vast scope and the general vagueness of the IT rules 2021, it wouldn't be surprising if we witness selective enforcement of some of the more stringent requirements.

Provisions under rule 5(1), which require the creation of a compliance team, can be abused to make requests for takedown of specific dissenting content. In time, this might either incentivise Facebook and Twitter to become increasingly compliant, providing the government more narrative control on their platforms, or result in the creation of more compliant homegrown alternatives.

Due to the possible uncertainty and volatility resulting from the IT rules (with only three months given to comply), a significant proportion of foreign investors are likely to be discouraged from investing in the digital intermediaries market. The potential cumulative effect could be a fall in the proportion of FDI in the Indian economy, with primarily government-backed domestic investors investing in an uncertain and heavily regulated digital intermediaries market. This effect could be even riskier, especially at a time when India is known to have lower investment freedom (a sign of higher uncertainty) in comparison to the global average, as shown in the graph below:



Source: 2021 Index of Economic Freedom, 1995-2021
Figure 2: Investment Freedom in India vs the world

Finally, even if not abused for surveillance purposes, the traceability requirement might not serve the public interest benefit expressed by the government. There is no denying that malicious WhatsApp forwards have caused mass panic, public unrest and loss of life in India. But traceability does not solve this problem. Digital intermediaries have shown that even simple acts such as sending a message can have dangerous outcomes, even when the parties' intentions are not malicious. For instance, it might be ineffective to hold individuals responsible for the violence that might have occurred in an area they have never lived in or heard of, simply because they created/disseminated a message as a joke or out of concern. The reasons behind public unrest over messaging content are complex. They have to do with both the architecture of platforms that enable the spread of information at great speed and the deep fault lines of Indian society that the content of viral forwards exploits. Such problems cannot be solved by holding first originators accountable.

Under the rule, if a certain message originates abroad, the first person to disseminate it in India would be considered the first originator. It is unclear how holding such a person accountable will be in the public interest, especially since a person cannot be aware that they are indeed the first originator of the information within the country.

The cross-posting of content is another hindrance. The same message can be sent across platforms, and therefore first originators on each platform are likely to be different. For instance, a viral forward on WhatsApp that is possibly held as the cause for violence could have been created by someone on Telegram or Instagram, from where the first originator of the content on WhatsApp could have picked it up. It is unclear how the movement of content between platforms can be monitored and how that might affect the first originator requirement. This might incentivise malicious actors to move to smaller platforms or create homebrew software for the initial dissemination of harmful content, from where the content can spread to larger ones.

Conclusion

The court's verdict on the traceability requirement is likely to have significant consequences not only on the future of privacy rights in India but also on the instant messaging and social media markets in the country. From our assessment of these consequences, we infer that the traceability requirement imposes disproportionate costs for what is, at best, an unclear "public interest" benefit.

End